KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40
regierungsrat@ag.ch
www.ag.ch/regierungsrat

Per E-Mail
Bundesamt für Justiz

cornelia.perler@bj.admin.ch

17. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Vernehmlassung

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 wurden die Kantonsregierungen zur Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) eingeladen. Der Regierungsrat des Kantons Aargau dankt Ihnen für die Gelegenheit. Er unterstützt die vorgesehenen Bestimmungen der VEKJ im Grundsatz und hat dazu die nachfolgenden Bemerkungen:

Artikel 4

Der Regierungsrat regt an, in Artikel 4 generell den Begriff "Datei" anstatt den Begriff "Dokument" zu verwenden. Aus technischer Sicht ist der Begriff "Datei" präziser als der Begriff "Dokument". "Dokument" beschreibt eher den fachlichen oder rechtlichen Inhalt, während für die technische Verarbeitung, Übermittlung, Speicherung, Virenprüfung und Formatvalidierung in erster Linie Dateien massgeblich sind. Es sollte deshalb geprüft werden, ob in den technisch geprägten Bestimmungen von Artikel 4 und den damit zusammenhängenden Vorschriften konsequent der Begriff "Datei" verwendet werden sollte.

Nach Absatz 2 können Beilagen grundsätzlich in jedem Format übermittelt werden. Der Regierungsrat erachtet diese Bestimmung nicht als sinnvoll, da der Informationsgehalt eines Dokuments in der Regel im Format PDF wiedergegeben werden kann. Die Beilagen sollen, wenn möglich, in diesem weit verbreiteten Format eingereicht werden, was die Fallbearbeitung durch die involvierten Stellen sowie die Verfahrensbeteiligten erleichtert. Zudem würde die uneingeschränkte Formatwahl ein erhebliches IT-Sicherheitsrisiko für alle Beteiligten darstellen. Insbesondere ist fraglich, ob gewährleistet ist, dass die zentrale Plattform sämtliche denkbaren Dateiformate einer Virenprüfung unterziehen kann. Absatz 2 könnte daher wie folgt lauten: "Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden." Würde die Offenheit betreffend Formate beibehalten werden, wäre dies nur dann sachgerecht, wenn dafür eine rechtliche oder verfahrensbezogene Notwendigkeit besteht, insbesondere wenn Originaldateien aufgrund ihres Beweiswerts, ihrer Struktur oder ihres Inhalts zwingend im Ursprungsformat eingereicht werden müssen. Ist eine solche juristische Notwendigkeit nicht gegeben, sollte die Einreichung auf wenige, standardisierte und sicher verarbeitbare Formate beschränkt werden. Dies dient der Interoperabilität, der Bearbeitbarkeit, der Langzeitverfügbarkeit und nicht zuletzt der IT-Sicherheit. Die uneingeschränkte Formatwahl würde ein erhebliches IT-Sicherheitsrisiko darstellen.

Die Liste der unterstützten Dateiformate in Absatz 3 ist vermutlich einem steten Wandel unterworfen. Zudem ist das reine Benennen von Formaten in der Verordnung nicht hinreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei verschlüsselten oder passwortgeschützten Elementen (zum Beispiel Makros in einer Microsoft Excel-Datei, ZIP-Dateien mit teilweise verschlüsselten Dateien etc.). Es sollte daher geprüft werden, ob die Festlegung der Formate und weitere technische Details nicht in einem Anhang zur VEKJ (durch das zuständige Departement anpassbar) oder einer Departementsverordnung geregelt werden sollen. Damit kann eine raschere Aktualisierung der technischen Details gewährleistet werden.

Gemäss Art. 2 Abs. 1 lit. c VEKJ soll die Plattform Dokumente bis zu zwei Gigabyte entgegennehmen und übermitteln können. Aus Sicht des Regierungsrats sollte klargestellt werden, dass die Systeme mindestens Dateien bis zu zwei Gigabyte verarbeiten können müssen und dass, soweit technisch und betrieblich sinnvoll, auch grössere Datenmengen ermöglicht werden können. Eine starre Obergrenze kann sich in der Praxis als zu restriktiv erweisen, namentlich bei multimedialen Inhalten, umfangreichen Verfahrensakten oder strukturierten Datensammlungen. Der Regierungsrat regt zudem an, auch die Speicher- und Grössenregeln separat und nicht in der VEKJ zu regeln. Die zulässigen Speichergrössen hängen von verschiedenen Faktoren ab, etwa von der technischen Architektur der Plattform, den Sicherheitsmechanismen, den Übertragungskapazitäten, den Prüfroutinen sowie den betrieblichen Rahmenbedingungen. Dadurch kann auf technische Entwicklungen und Betriebserfahrungen flexibler reagiert werden.

Artikel 6

In den Erläuterungen wird ausgeführt, dass gemäss Art. 22 Abs. 2 des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) verfahrensleitende und verfahrensbeteiligte Behörden verpflichtet seien, ihre Mitteilungen zu siegeln und mit einem Zeitstempel zu versehen. Unserer Ansicht nach sollten verfahrensbeteiligte Behörden nicht verpflichtet werden, ihre Dokumente elektronisch zu siegeln. Andernfalls müssten alle Schweizer Behörden auf allen Stufen mit einem Siegel ausgestattet werden. Für die Kantone wäre eine flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden. Art. 22 Abs. 2 BEKJ ist daher einschränkend auszulegen; nur die verfahrensleitende Behörde wird verpflichtet, ihre Dokumente elektronisch zu siegeln. Die Erläuterungen sollten dahingehend angepasst werden. Darüber hinaus sollte geprüft werden, ob Art. 6 VEKJ entsprechend präzisiert werden soll.

Artikel 7

Absatz 1 regelt die Siegelung durch die Plattform für den Fall, dass mehrere Dokumente eingereicht werden. Unklar ist jedoch, wie gesiegelt wird, wenn nur ein Dokument übermittelt wird. Wird das Siegel in diesem Fall auf dem eingereichten Dokument oder in einem separaten Dokument angebracht? Die Erläuterungen sollten sich hierzu klar äussern. Falls das übermittelte Dokument nie gesiegelt wird, wäre Absatz 1 entsprechend anzupassen.

Artikel 12

Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein "Briefkasten" und keine Langzeitablage sein soll. Bei den Quittungen scheint es dagegen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Quittungen können erst spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Die Behörden müssen zwar darum besorgt sein, die Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch aufgrund der Funktionsweise der zentralen Plattform – etwa im Fall von Zustellungen – dazu kommen, dass das Herunterladen der Quittungen unterbleibt.

Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von der Plattform selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen. Quittungen sollten daher – in Anlehnung an die Zeitspanne, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind – erst nach drei Jahren gelöscht werden.

Artikel 14

Auf die in Absatz 1 beziehungsweise Absatz 2 geregelte Festlegung der (Maximal-)Grösse von prüfbaren Blöcken grösserer Dateien sollte verzichtet werden. Vielmehr sollte dieser Grenzwert basierend auf den technischen Möglichkeiten, den verfügbaren Prüfmechanismen und der zunehmenden Betriebserfahrung der Plattformbetreiber angepasst und bei Bedarf erhöht werden können. Eine flexible Regelung erscheint zweckmässiger als eine starre Festlegung im Normtext. Damit kann sowohl dem Stand der Technik als auch der Weiterentwicklung von Sicherheitslösungen Rechnung getragen werden. Die vorgesehene Regelung eröffnet potenziellen Angreifern die Möglichkeit, ihre Schadsoftware in einer verseuchten Datei so anzuordnen, dass der Schadcode bei der Aufspaltung in mehrere Blöcke in zwei aufeinanderfolgenden Blöcken liegt und nicht zuverlässig als schädlich erkannt werden kann. Der Grenzwert für eine vollständige Prüfung auf Schadsoftware von derzeit 64 MB sollte sodann basierend auf den technischen Möglichkeiten und der wachsenden Betriebserfahrung durch die Betreiber der Plattformen erhöht werden können. Absatz 1 sollte daher lediglich festhalten, dass die Plattformen eine Virenprüfung durchführen müssen. Absatz 2 kann gestrichen werden.

Für allfällige Rückfragen steht Ihnen Herr Rudolf Moos, Stabsmitarbeiter im Departement Volkswirtschaft und Inneres (rudolf.moos@ag.ch; 062 835 14 14), gerne zur Verfügung.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Stephan Attiger
Landammann

Joana Filippi
Staatsschreiberin

Appenzell Ausserrhoden

Regierungsrat

Obstmarkt 3
9102 Herisau
Tel. +41 71 353 61 11
kantonskanzlei@ar.ch
www.ar.ch

Regierungsrat, 9102 Herisau

Eidg. Justiz- und Polizeidepartement
3003 Bern

Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 11. Juni 2026

Eidg. Vernehmlassung; Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 unterbreitete das Eidgenössische Justiz- und Polizeidepartement die eingangs erwähnte Vorlage zur Vernehmlassung. Die Vernehmlassungsfrist dauert bis zum 22. Juni 2026.

Allgemeine Bemerkungen

Der Regierungsrat hält fest, dass die digitale Transformation der Schweizer Justiz grundsätzlich zu unterstützen ist. Die schweizweiten Bemühungen in dieser Hinsicht sind weit fortgeschritten, die verschiedenen elektronischen Systeme werden bereits in Pilotprojekten getestet. Die Zusammenarbeit des Bundes und der Kantone hat sich in dieser Sache bewährt.

Der Regierungsrat beurteilt den Vorentwurf der VEKJ positiv. Der Entwurf konkretisiert die im BEKJ angelegte Stossrichtung und schafft eine einheitliche Grundlage für die rechtssichere elektronische Kommunikation im staatlichen Kontext. Aus prozessualer Sicht kann die vorgesehene Lösung die Voraussetzungen für eine durchgängige, medienbruchfreie Digitalisierung von Verfahren schaffen, insbesondere durch die rechtssichere elektronische Zustellung sowie die standardisierte Abwicklung von Eingaben und Rechtsmitteln. Die in der Verordnung vorgesehenen Schnittstellen schaffen klare Ansatzpunkte für die Anbindung bestehender Systeme.

Der Regierungsrat vermisst jedoch klärende Ausführungen dazu, wie bei den Plattformen die vorgesehene durchgängige Verschlüsselung der Daten (nicht nur «in-transit», sondern auch «at-rest») mit der ebenfalls vorgesehenen Virenprüfung zusammengehen soll. Eine wirksame Virenprüfung dürfte aus Sicht des Regierungsrates nur auf entschlüsselten Daten stattfinden können. Eine ähnliche Problematik gibt es z.B. im Bereich der automatisierten Erkennung von verbotener Pornographie in verschlüsselter Kommunikation.

In finanzieller Hinsicht stellt der Regierungsrat fest, dass die Aufteilung der wiederkehrenden Kosten zwischen Bund und Kantonen grundsätzlich nachvollzogen werden kann (vgl. S. 28 des erläuternden Berichts). Um die wiederkehrenden Kosten für den Betrieb und die Weiterentwicklung beurteilen zu können, sollten die gesamten Investitionskosten dargelegt werden. Weiter regt der Regierungsrat an, drei bis vier Jahre nach der Inbetriebnahme einen Bericht über die Einführung und deren Auswirkungen zu erstellen. In diesem Zusammenhang könnte auch geprüft werden, ob die Digitalisierung in der Justiz zu Effizienzgewinnen geführt hat, wie dies im erläuternden Bericht (S. 28) in Aussicht gestellt wird.

Insoweit dem EJPD in der VEKJ das Recht zugestanden wird, selbständig weitere Detail-Regelungen zu erlassen, fordert der Regierungsrat vorgängig ein Vernehmlassungsverfahren; im Rahmen dessen sich die Kantone unter Einbezug der direkt betroffenen kantonalen Stellen äussern können.

Im Verordnungsentwurf ist mehrfach die Rede von «Behörden». Was der Begriff genau umfasst, ist jedoch nicht ohne weiteres klar. Offene Fragen sollten sich, wenn möglich, basierend auf die VEKJ beantworten lassen und nicht erst im Nachhinein durch die Rechtsprechung geklärt werden müssen.

Bemerkungen zu den einzelnen Artikeln

Die folgenden Artikel geben aus Sicht des Regierungsrates zu Fragen und Bemerkungen Anlass:

Art. 2 Anforderungen an die Plattformen

Die Anforderungen an die Plattformen scheinen sachgerecht. Aufgrund der schnellen technischen Entwicklung sollte die maximale Dateigrösse gemäss Absatz 1 Buchstabe c jedoch in einem Anhang zur vorliegenden Verordnung oder in einer Departementsverordnung des EJPD festgelegt werden. Gemäss erläuterndem Bericht (S. 11) können die Betreiberinnen von Plattformen in die Übermittlung von Dokumenten, die grösser als die festgelegte Maximalgrösse sind, einwilligen, wobei die Einwilligung mündlich oder schriftlich erfolgen kann. Die kantonalen Nutzer der Plattform sehen sich im Bereich von Strafverfahren immer wieder mit der Übermittlung von Abbildern von beschlagnahmten Computern oder Mobiltelefonen konfrontiert, welche obige Datenbegrenzung überschreiten dürften, weshalb der Regierungsrat eine unbürokratische und rasche Einwilligung in die Übermittlung von grösseren Datenmengen begrüsst; namentlich befürwortet er, dass die Bewilligung «in dringenden Fällen» vorab auch mündlich erteilt werden kann.

Art. 4 Format der Dokumente

Der Vorentwurf verwendet – wie das BEKJ – den Begriff «Dokument» anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: «Der Begriff "Datei" ist für das Gesetz zu technisch.» In diesem Sinne ist in der Verordnung der Begriff Datei – an Stelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

Abs. 2
Nach den heutigen Weisungen über das Archivwesen werden nicht nur die Gerichtsakten (z.B. Rechtsschriften, Protokolle, Gutachten, Urteile), sondern auch die Beilagen, welche im Verlauf des Verfahrens in Fotokopie eingereicht wurden, archiviert; lediglich die Originale werden an die Parteien retourniert (vgl. Ziff. 1.3 i. V. m. Ziff .3.4 der Weisung über das Archivwesen der Gerichte und weiterer Justizbehörden vom 31. Januar 2016). Mit Blick auf diesen Umstand stellt sich die Frage, ob nicht auch die Beilagen zwingend in einem Format

eingereicht werden sollten, welches sich für eine «Langzeitarchivierung» eignet (namentlich PDF/A). Es besteht ansonsten die Gefahr, dass das Kanzleipersonal der kantonalen Nutzer der Plattform vor der Archivierung in mühsamer Arbeit ungeeignete Formate «konvertieren» muss.

In Einzelfällen kann das Format PDF/A den Informationsgehalt eines Dokuments nicht genügend wiedergeben. Zu denken ist beispielsweise an Audio- oder Videoaufnahmen, an mehrspurige Tunnelüberwachungen oder Aufzeichnungen aus Elektroautos. Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattformen übermittelt werden können. Aus Sicherheitsgründen scannt die zentrale Plattform alle Dateien auf Viren. Dabei kann die zentrale Plattform grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Für Dokumente, welche nicht direkt über die Plattformen übermittelt werden dürfen, besteht die Möglichkeit zur Übermittlung in einem Container, beispielsweise als Zip-Format.

Welche Dateiformate die Plattformen verarbeiten müssen, ist durch das EJPD nach Anhörung der Betreiberin der zentralen Plattform in einer Departementsverordnung zu regeln.

Absatz 2 sollte daher wie folgt lauten:
[2] ~~Die Beilagen können in jedem Format übermittelt werden.~~ Ist das Format PDF/A ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden.

Abs. 3, 4 und 5
Die vorgeschlagene Auswahl der Dateiformate wird begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen. Da die Länge der Frist, die Beilage in einem von der Behörde festgelegten Format einzureichen, im Einzelfall durch die Verfahrensleitung festzulegen ist, geht der Regierungsrat davon aus, dass es sich hierbei um eine richterliche Frist handelt, welche aus zureichenden Gründen erstreckt werden kann (vgl. Art. 144 Abs. 2 ZPO).

Art. 5 Quittungen

Die vorgeschlagene Regelung wird begrüsst. Es ist wichtig, dass der Name der verantwortlichen Person einer Behörde gemäss Art. 5 Abs. 2 Bst. b in der Quittung nicht aufgeführt wird. Nur der Name der Behörde sollte auf der Quittung erscheinen. Die Plattformen müssen künftig auch strukturierte Daten übermitteln können, beispielsweise in Form von XML-Dateien. Die Ausnahmen in den Absätzen 4 und 5 sind daher wesentlich, da XML-Dateien aus technischen Gründen nicht gesiegelt werden können.

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Die Authentifizierung über AGOV gemäss Absatz 1 ist sinnvoll und zielführend. Die detaillierten Anforderungen sollten in einer Departementsverordnung des EJPD geregelt werden. Der mögliche Einsatz von zusätzlichen Authentifizierungsdiensten bei künftigen kantonalen Plattformen gemäss Absatz 2 wird begrüsst. Künftig sind die meisten Behörden über eine Schnittstelle mit der zentralen Plattform verbunden. Absatz 3 lässt genügend Spielraum, um künftige technische Lösungen umzusetzen.

Art. 9 Profile

Abs. 2
Diese Bestimmung bezieht sich einzig auf verfahrensleitende Behörden, die auch im Adressverzeichnis der zentralen Plattform erscheinen. Bei verfahrensleitenden Behörden ist auf die Angabe einer postalischen Adresse zu verzichten, da eine Behörde über mehrere Standorte und verschiedene Postadressen verfügen kann. Die Bestimmung ist entsprechend anzupassen.

Abs. 4
Der Sinn von Absatz 4 ist nicht verständlich. Es ist unklar, ob sich die Pflicht zur elektronischen Übermittlung auf die natürliche Person oder die Organisation, für welche die natürliche Person tätig ist, bezieht. Letzteres dürfte der Fall sein. Die Formulierung von Absatz 4 ist entsprechend zu präzisieren. Im erläuternden Bericht wird die verantwortliche Person einer Organisation erwähnt. Es ist wünschenswert, dass die Rolle der verantwortlichen Person in Bezug auf die zentrale Plattform in der Verordnung geklärt wird.

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Art. 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein «Briefkasten» und keine Langzeitablage sein soll. Bei den Quittungen scheint es dagegen angezeigt, eine längere Aufbewahrungsfrist von drei Jahren vorzusehen. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen.

Die Verlängerung der gesetzlichen Mindestfrist von 90 Tagen auf die maximale Dauer von sechs Monaten für die Aufbewahrung von Daten auf der Plattform ist aus Sicht des Regierungsrates kein Nachteil.

Art. 16 Aufteilung der Gebühr

Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 % wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die Aufteilung der Gebühr sollte Gegenstand der Prüfung sein. Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen.

Art. 22a (neu) Rücksendung von physischen Dokumenten

Problemstellung:
Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen in Papierform eingehen, weil derlei Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst

auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender. Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es in der analogen Welt noch gar nicht gab. Dies kann nicht der Willen des Gesetzgebers gewesen sein.

Lösungsansatz:
Aus den oben genannten Gründen schlägt der Regierungsrat vor, einen neuen Art. 22a einzufügen. Die gewählte Formulierung stellt klar, dass Dokumente, die gemäss Art. 30 Abs. 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Art. 30 BEKJ in die Verordnung aufzunehmen. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen:

2. Kapitel: *Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten*

[…]

Art. 22a Rücksendung von physischen Dokumenten
Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.

Art. 22b (neu) Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten

Art. 22 konkretisiert Art. 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde. Wo sich Private nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird. Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von 10 bis 20 % der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Lösungsansatz:
Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Aus den in Ziffer 3.1 genannten Gründen wird deshalb vorgeschlagen, einen neuen Art. 22b einzufügen:

Art. 22b *Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten*

Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.

Sollte an der viel zu engen Auslegung des BEKJ festgehalten werden, die im erläuternden Bericht skizziert ist, wäre zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen, um dem in den Verfahrensgesetzen verwendeten Begriff der «Unterschrift» genüge zu tun, obwohl diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung durch das Behördensiegel ersetzt wurde.

Art. 28 Inkrafttreten

Die Finanzierung des Projekts Justitia 4.0, welches die zentrale Plattform im Auftrag der Kantone, des Bundes und der Justizbehörden aufbaut, ist bis Ende Jahr 2027 gesichert. Die Finanzierung von Betrieb und Weiterentwicklung der zentralen Plattform muss daher spätestens ab Anfang 2028 über Gebühren erfolgen. Die Verordnung muss gleichzeitig mit dem abschliessenden Inkrafttreten des BEKJ in Kraft gesetzt werden.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Roger Nobs, Ratschreiber

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
cornelia.perler@bj.admin.ch

Appenzell, 3. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie uns die Vernehmlassungsunterlagen zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie verzichtet auf eine Stellungnahme.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Roman Dobler

Zur Kenntnis an:
- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

Landeskanzlei
Rathausstrasse 2
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bern

cornelia.perler@bj.admin.ch

Liestal, 9. Juni 2026

Vernehmlassung betreffend Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat

Besten Dank für die Gelegenheit zur Meinungsäusserung. Wir unterstützen den Verordnungsentwurf grundsätzlich. Inhaltlich schliessen wir uns der Musterstellungnahme von justitia 4.0 an, die Sie in der Beilage finden.

Hochachtungsvoll

Dr. Anton Lauber
Regierungspräsident

E. Heer Dietrich

Elisabeth Heer Dietrich
Landschreiberin

– Musterstellungnahme justitia 4.0

Vernehmlassung: Vorentwurf zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VE-VEKJ)

Arbeitshilfe zur Vorbereitung der Stellungnahme für kantonale Behörden

An seiner Sitzung vom 13. März 2026 hat der Bundesrat die Vernehmlassung zum Vorentwurf der VEKJ (VE-VEKJ) eröffnet. Eine Stellungnahme kann bis am 22. Juni 2026 eingereicht werden.

Die vorliegende Arbeitshilfe dient der Unterstützung der kantonalen Behörden und weiteren interessierten Kreise zur Erarbeitung ihrer Stellungnahme. Sie beinhaltet im Wesentlichen Erläuterungen und Anregungen zu den einzelnen Verordnungsartikeln sowie Formulierungsvorschläge, stellt jedoch nicht die Stellungnahme des Projektes Justitia 4.0 dar.

Autorinnen und Autoren

Kantonale Behörden: Alexandra Altherr Müller, Sozialversicherungsgericht ZH, Patrick Becker, Justizleitung GE, Jan Grunder, Regionalgericht Oberland BE, Stéphane Nakamura, Bezirksgericht Greyerz FR, Marc Tille, Rechtsdienst für Sicherheit und Justiz VS, Serge Segura, Kantonsgericht VD, Daniel Stehlin, Staatsanwaltschaft BL, Stephan Walder, Oberstaatsanwaltschaft ZH, André Zumthurm, Kantonsgericht LU

Projektteam Justitia 4.0: Jérôme Barraud, Chantal Neuschwander, Christian Renggli, Houri Rousseau

Erläuterungen, Anregungen und Formulierungsvorschläge

Ingress

Im Vorentwurf fehlen bewusst die Artikel, die dem Bundesrat die Kompetenz zur Regelung des Formats der elektronisch übermittelten Dokumente übertragen. Im erläuternden Bericht wird präzisiert, dass, "um die Übersichtlichkeit zu bewahren", im Ingress lediglich die Bestimmungen der Verfahrensgesetze erwähnt werden, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben. Auch wenn ein allgemeiner Verweis auf das BEKJ angemessen erscheint, wäre es vorzuziehen, alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen. Dies gilt insbesondere für die Artikel, die dem Bundesrat die Kompetenz zur Festlegung der Formate übertragen; diese sollten daher logischerweise ebenfalls im Ingress erwähnt werden.

Der Ingress sollte daher wie folgt ergänzt werden:

> *Der Schweizerische Bundesrat,*
>
> *gestützt auf das Bundesgesetz vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ),*
>
> *die Artikel 6a Absatz 2, 21a Absatz 2 und 34 Absatz 1bis des Verwaltungsverfahrensgesetzes vom 20.Dezember 1968 (VwVG),*
>
> *Artikel 38e des Bundesgerichtsgesetzes vom 17. Juni 2005 (BGG),*
>
> *die Artikel 128b Absatz 3, 128c Absatz 2 und 128e der Zivilprozessordnung (ZPO),*
>
> *die Artikel 33a Absatz 4, 33b, 33c Absatz 2 und 34 Absatz 3 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG),*
>
> *die Artikel 76a Absatz 2, 103b Absatz 3, 103c Absatz 2 und 103e der Strafprozessordnung (StPO),*
>
> *Artikel 2e des Bundesgesetzes vom 23. Dezember 2011 über den ausserprozessualen Zeugenschutz (ZeugSG),*
>
> *Artikel 31f des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR),*
>
> *die Artikel 8c Absatz 3, 8d Absatz 2 und 8f des Opferhilfegesetzes vom 23. März 2007 (OHG)*

und die Artikel 37d und 38a Absatz 2 des Militärstrafprozesses vom 23. März 1979 (MStP), verordnet:

1. Kapitel: Betrieb und Nutzung von Plattformen

1. Abschnitt: Geltungsbereich

Art. 1

Absatz 2 betrifft ausschliesslich bundesrechtliche Verfahren nach VwVG und ist **daher für die Kantone nicht relevant**. Unklar scheint der Mehrwert von **Absatz 3**, gehen Gesetze dieser Verordnung doch ohnehin vor.

2. Abschnitt: Betriebsbewilligung

Art. 2 Anforderungen an die Plattformen

Die Anforderungen an die Plattformen scheinen sachgerecht. Aufgrund der schnellen technischen Entwicklung sollte die maximale Dateigrösse gemäss **Absatz 1 Buchstabe c** jedoch in einem Anhang zur vorliegenden Verordnung oder in einer Departementsverordnung des EJPD festgelegt werden.

Die **Löschfunktion in Absatz 1 Buchstabe d ist eine Funktionalität**, welche – wenn überhaupt - im 3. Abschnitt dieser Verordnung geregelt werden sollte. Zudem ist der Wortlaut der Bestimmung zu absolut formuliert und kaum umsetzbar. Wie der erläuternde Bericht auf Seite 11 zurecht ausführt, wird durch die Löschfunktion die erteilte individuelle Berechtigung gelöscht, nicht jedoch das Dokument als solches. Zudem wäre bei der Löschung zwischen den Behörden und anderen Nutzern zu unterschieden.

Art. 3 Bewilligungsverfahren

Keine Bemerkungen.

3. Abschnitt: Dokumente, Quittungen und Siegelung

Art. 4 Format der Dokumente

Der Vorentwurf verwendet – wie das BEKJ – den Begriff "Dokument" anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: "Der Begriff "Datei" ist für das Gesetz zu technisch."

In diesem Sinne ist in der Verordnung der Begriff Datei – an Stelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

Abs. 1

Die Festlegung des Formats PDF/A für Dokumente von Behörden und der Formate PDF und PDF/A für die übrigen Verfahrensbeteiligten wird begrüsst.

Abs. 2

In vielen Fällen kann der Informationsgehalt eines Dokuments im Format PDF rechtsgenüglich wiedergegeben werden. Insofern soll die Beilage in diesem weit verbreiteten Format eingereicht werden, was die Fallbearbeitung durch die Anwältinnen und Anwälte, die Staatsanwaltschaften, die Gerichte, die Verwaltungsbehörden und durch die weiteren Verfahrensbeteiligten erleichtert. Reichen die Verfahrensbeteiligte ihre Beilagen im Format PDF ein, entfällt die Konversion durch die Justizbehörden, allen Beteiligten liegt das gleiche Dokument vor. Die Digitalisierung soll die Verfahren beschleunigen und die Aktenführung vereinfachen. Wenn Dokumente im Regelfall als PDF-Dokument vorliegen, ermöglicht dies eine speditive Bearbeitung durch die Anwaltschaft und die Behörden. Geschäftsverwaltungssysteme der Anwältinnen, Anwälte und Behörden können aus Sicherheitsgründen nur mit einer beschränkten Anzahl an Dateitypen umgehen ('Whitelistening' von Fileformaten). Wenn das Format der Beilagen frei gewählt werden könnte,

würde dies die Fallbearbeitung erheblich erschweren. Alle Verfahrensbeteiligten müssten zuerst nach dem passenden Programm suchen, um eine Datei zu öffnen. Zudem würde die uneingeschränkte Formatwahl ein erhebliches IT-Sicherheitsrisiko für alle Beteiligten darstellen.

In Einzelfällen kann das Format PDF den Informationsgehalt eines Dokuments nicht genügend wiedergeben. Zu denken ist beispielsweise an Audio- oder Videoaufnahmen, an mehrspurige Tunnelüberwachungen oder Aufzeichnungen aus Elektroautos. Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattformen übermittelt werden können. Aus Sicherheitsgründen scannt die zentrale Plattform alle Dateien auf Viren. Dabei kann die zentrale Plattform grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Für Dokumente, welche nicht direkt über die Plattformen übermittelt werden dürfen, besteht die Möglichkeit zur Übermittlung in einem Container, beispielsweise als Zip-Format.

Welche Dateiformate die Plattformen verarbeiten müssen, ist durch das EJPD nach Anhörung der Betreiberin der zentralen Plattform in einer Departementsverordnung zu regeln.

Absatz 2 sollte daher wie folgt lauten:

> [2] ~~*Die Beilagen können in jedem Format übermittelt werden.*~~ *Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden.*

Abs. 3 und 4

Die vorgeschlagene Auswahl der Dateiformate wird begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen.

Die Liste der unterstützten Dateiformate ist einem stetigen Wandel unterworfen. Es sind daher häufige Anpassungen zu erwarten. Zudem ist das reine Benennen von Formaten in der Verordnung nicht hinreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei dennoch verschlüsselten oder passwortgeschützten Elementen (z.B. Makros in einer Microsoft Excel-Datei, ZIP-Dateien mit teilweise verschlüsselten Dateien etc.). Dies ist in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung.

Absätze 3 und 4 sollten daher wie folgt lauten:

> [3] ~~*Die verfahrensleitende Behörde muss folgende Formate bearbeiten können:*~~
>
> ~~*a. schriftliche Unterlagen: PDF, PDF/A;*~~
>
> ~~*b. Bilddateien: BMP, GIF, JPEG, PNG;*~~
>
> ~~*c. Audiodateien: MP3, OGG, WAV;*~~
>
> ~~*d. Videodateien: AVI, MOV, MKV, MP4;*~~
>
> ~~*e. Archivdateien: ZIP, 7z.*~~
>
> *Kann die verfahrensleitende Behörde eine Beilage im Format, in dem sie eingereicht wurde, nicht öffnen, so räumt sie der einreichenden Partei eine angemessene Frist ein, damit diese die Beilage in einem von der Behörde festgelegten Format einreichen kann.*
>
> [4] ~~*Wird eine Beilage in einem anderen Format eingereicht und kann die verfahrensleitende Behörde die Beilage nicht zweckmässig bearbeiten, so fordert sie die einreichende Person oder Behörde auf, die Beilage in einem von der verfahrensleitenden Behörde festgelegten Format einzureichen oder den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen.*~~ *Das EJPD regelt die über die Plattformen zu übertragenden Dateiformate.*
>
> [5] ~~*Sie räumt ihr eine angemessene Frist ein.*~~

Art. 5 Quittungen

Die vorgeschlagene Regelung wird begrüsst. Es ist wichtig, dass der **Name der verantwortlichen Person einer Behörde** gemäss Absatz 2 Buchstabe b in der Quittung **nicht** aufgeführt wird. Nur der Name der Behörde sollte auf der Quittung erscheinen.

Absatz 2 Buchstabe d konkretisiert die Eingangsquittung und gibt unter anderem vor, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung aufzulisten sind. Mögliche Gründe für eine Rückweisung durch die Plattform sind ein positives Resultat bei der Virenprüfung, die Dateigrösse oder ein Dateiformat, welches die Plattform nicht erkennt.

Absatz 2 Buchstabe d Ziffer 2 präzisiert, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung auszuweisen bzw. aufzulisten sind. Die Bestimmung enthält einen logischen Fehler: Nicht übermittelte Dokumente können auf der **Eingangsquittung** nicht aufgeführt werden, da diese eben **nicht übermittelt** wurden. Die Quittung kann keine Hashwerte von Dateien enthalten, welche nicht übermittelt worden sind. Kann die Plattform ein oder mehrere Dokumente nicht übermitteln, so erhält die Absenderin oder der Absender eine Mitteilung der Plattform, jedoch keine Quittung. Die Ziffer 2 ist daher zu streichen:

[2] Die Quittungen müssen insbesondere folgende Angaben enthalten:

a. die Art der Quittung;

b. den Namen der Absenderin oder des Absenders, ihre oder seine Adresse auf der Plattform und gegebenenfalls den Namen oder die Firma der Organisation, für welche die Absenderin oder der Absender handelt;

c. den Namen oder die Firma der Adressatin oder des Adressaten sowie ihre oder seine Adresse auf der Plattform;

d. bei einer Eingangsquittung:

1. die Liste der übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte,

~~2. die Liste der aufgrund des Resultats der Virenprüfung nicht übermittelten Dokumente und deren Grösse,~~

~~3.~~2. den Zeitpunkt der Übermittlung an die Plattform;

e. bei einer Abrufquittung: den Zeitpunkt des erstmaligen Abrufs;

f. bei einer Nichtabholquittung: den Zeitpunkt der Übermittlung an die Plattform;

g. beim Versand oder erstmaligen Abruf aufgrund der Weitergabe einer Berechtigung: den Namen der Person, in deren Name der Versand oder Abruf erfolgt.

Die Plattformen müssen künftig auch strukturierte Daten übermitteln können, beispielsweise in Form von XML-Dateien. Die Ausnahmen in den Absätzen 4 und 5 sind daher wesentlich, da XML-Dateien aus technischen Gründen nicht gesiegelt werden können.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Im elektronischen Rechtsverkehr wird das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben. Die Plattform dagegen bringt ihr Siegel **nach** der Übermittlung auf die Plattform auf der ausgestellten Eingangsquittung gestützt auf Artikel 5 an.

Artikel 6 regelt die **Sieglung der Dokumente** durch die verfahrensleitende Behörde **vor der Übermittlung über eine Plattform** (Art. 22 Abs. 2 BEKJ). Der Vorentwurf führt aus, dass bei der Übermittlung von mehreren Dokumenten die Sieglung eines Dokuments genüge. Dies ist korrekt. Zu ergänzen ist, dass die Siegelung durch die verfahrensleitende Behörde unabhängig von der Anzahl der übermittelten Dokumente erfolgt. Auch ein einzelnes Dokument, welches die verfahrensleitende Behörde übermittelt, muss gesiegelt werden, damit die Authentizität des Dokuments unabhängig von einer Plattform überprüft werden kann.

Die Ausführungen im erläuternden Bericht, wonach eine Behörde alle Dokumente mit einem Siegel versehen muss, widersprechen dem Wortlaut der Verordnung: Die Siegelung eines Dokuments durch die verfahrensleitende Behörde genügt. Zudem entspricht die Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden nicht dem technischen Konzept der zentralen Plattform.

Die **Unterscheidung zwischen verfahrensleitenden und verfahrensbeteiligten Behörden** ist für verschiedene Funktionalitäten der zentralen Plattform essenziell. Beispielsweise können nur verfahrensleitende Behörden Zustellungen vornehmen. Nur die Adresse von verfahrensleitenden Behörden ist für Drittpersonen aus dem öffentlichen Verzeichnis der zentralen Plattform ersichtlich. Würde an der Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden festgehalten, könnten alle Behörden uneingeschränkt und verfahrensunabhängig Zustellungen an andere Behörden, Organisationen und Privatpersonen vornehmen. Dies würde die zentrale Plattform für jegliche elektronische Kommunikation zwischen Behörden öffnen, wofür das BEKJ jedoch keine hinreichende gesetzliche Grundlage liefert. Sinn und Zweck des BEKJ ist es, die elektronische Kommunikation in Justizverfahren zu ermöglichen.

Nur verfahrensleitende Behörden sind verpflichtet, ihre Dokumente elektronisch zu siegeln. Artikel 22 Absatz 2 BEKJ ist daher einschränkend auszulegen. Das elektronische Siegel stellt die Herkunft, den Zeitpunkt, die Integrität und die Authentizität des gesiegelten Dokuments sicher. Die Verfügung oder der Entscheid einer verfahrensleitenden Behörde begründen Rechte und Pflichten und entfalten Wirkung über das einzelne Verfahren hinaus. Betroffene müssen daher unabhängig von einem konkreten Verfahren oder von der zentralen Plattform prüfen können, ob das fragliche Dokument integer und authentisch ist und von der dafür zuständigen Behörde erstellt wurde. Das elektronische Siegel ist zusammengefasst genau dort notwendig, wo Behörden autoritativ auftreten.

Verfahrensbeteiligte Behörden dagegen dürfen nicht verpflichtet werden, ihre Dokumente zu siegeln. Die Dokumente, welche verfahrensbeteiligte Behörden in einem Justizverfahren übermitteln, begründen in der Regel keine neuen Rechte und Pflichten. Typischerweise handelt es sich bei diesen Dokumenten um Auszüge aus bestehenden Registern, Auszüge aus bestehenden Akten früherer Verfahren, bereits eröffnete Verfügung oder Entscheide aus abgeschlossenen Verfahren, welche nun für ein Justizverfahren zur Verfügung gestellt werden. Die Authentifizierung auf der zentralen Plattform ermöglicht die korrekte Identifikation der Behörde. Will ein Verfahrensbeteiligter die Integrität oder Authentizität eines von einer verfahrensbeteiligten Behörde übermittelten Dokuments in Frage stellen, ist dies eine Frage der Beweiswürdigung im entsprechenden Verfahren.

Würde an der Siegelpflicht für alle Behörden gemäss erläuterndem Bericht festgehalten, so müssten alle Schweizer Behörden auf allen Stufen mit einem Siegel ausgestattet werden. Für die flächendeckende Ausstattung aller Schweizer Behörden mit einem elektronischen Siegel liefert das BEKJ keine genügende gesetzliche Grundlage. Für die Kantone wäre zudem eine flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden.

Gemäss erläuterndem Bericht müssen Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, nicht mehr gesiegelt werden. Diese Aussage entspricht nicht dem Konzept des BEKJ. Das BEKJ schreibt keine Funktionalität vor, wonach die zentrale Plattform qualifizierte elektronische Signaturen von Behördenmitgliedern einer Behörde zuordnet. Aus diesem Grund müssen verfahrensleitende Behörden Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, vor dem Versand über die Plattform standardmässig mit ihrem Siegel versehen.

Es müsste hingegen geklärt werden, wie Behörden Dokumente unterzeichnen können, die gemäss gegenwärtiger Rechtsprechung eine Unterschrift der Autorenschaft tragen müssen, so etwa Sachverständi-

gengutachten (BSK StPO-Heer, Art. 187 N 1). Diese können etwa im Fall von rechtsmedizinischen Instituten oder im Fall des Eidgenössischen Instituts für Metrologie METAS durchaus auch von Behörden oder zumindest von "Amtsstellen" erbracht werden. In diesen Fällen ist es erheblich, welche sachverständige Person das Gutachten erstattet, weshalb die qualifizierte elektronische Signatur (entgegen der Kommentierung zu Art. 22 BEKJ in der Botschaft, BBl 2023 679, S. 30), möglicherweise auch inskünftig noch zur Anwendung gelangen müsste.

Wichtig zu ergänzen ist die Unterscheidung zwischen Versand und Akteneinsicht. Bei der Akteneinsicht besteht, wie der erläuternde Bericht zu Artikel 7 ausführt, dagegen keine Pflicht zur Siegelung der Dokumente durch die verfahrensleitende Behörde.

Art. 7 Siegelung der Dokumente durch die Plattformen

Im elektronischen Rechtsverkehr soll das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt werden. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben (Art. 6). Artikel 7 bezieht sich dagegen auf die Siegelung der Quittung **nach** der Übermittlung durch die zentrale Plattform.

Abs. 1

Der Grundsatz der Siegelung durch die Plattformen wird im Vorentwurf korrekt wiedergegeben: Träger des Siegels der Plattform ist die **Quittung, nie das übermittelte Dokument.** Im Falle der zentralen Plattform handelt es sich dabei um die sogenannte Eingangs- oder Abrufquittung. Die zentrale Plattform siegelt die Quittungen der Benutzerinnen und Benutzer, unabhängig davon, ob sie ein oder mehrere Dokumente übermitteln. Absatz 1 sollte daher wie folgt lauten:

> [1] *Werden ~~mehrere~~ Dokumente ~~zusammen~~ übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an. Das Dokument muss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.*

Abs. 2

Absatz 1 beschreibt die Siegelung der Quittungen. Die Übermittlung von gesiegelten Dokumenten folgt den gleichen Regeln wie in Absatz 1. **Absatz 2 muss daher gestrichen werden**.

> ~~[2] *Dokumente, die bereits über ein Siegel oder eine qualifizierte elektronische Signatur mit einem Zeitstempel verfügen, müssen nicht erneut mit einem Siegel versehen werden.*~~

4. Abschnitt: Authentifizierung, Profile, Schnittstellen und Berechtigungen

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Die Authentifizierung über AGOV gemäss Absatz 1 ist sinnvoll und zielführend. Die detaillierten Anforderungen sollten in einer Departementsverordnung des EJPD geregelt werden.

Der mögliche Einsatz von zusätzlichen Authentifizierungsdiensten bei künftigen kantonalen Plattformen gemäss Absatz 2 wird begrüsst.

Künftig sind die meisten Behörden über eine Schnittstelle mit der zentralen Plattform verbunden. Absatz 3 lässt genügend Spielraum, um künftige technische Lösungen umzusetzen.

Art. 9 Profile

Abs. 2

Diese Bestimmung bezieht sich einzig auf verfahrensleitende Behörden, die auch im Adressverzeichnis der zentralen Plattform erscheinen. Bei verfahrensleitenden Behörden ist auf die Angabe einer postalischen Adresse zu verzichten, da eine Behörde über mehrere Standorte und verschiedene Postadressen verfügen kann. Die Bestimmung ist entsprechend anzupassen.

[2] *Die Profile von Behörden müssen mindestens folgende Angaben enthalten:*

a. Name der Behörde;

~~b. Postadresse;~~

~~c~~ b. Bezeichnung ihres Siegels.

Abs. 3 Bst. a

Die Übernahme des Geburtsdatums aus dem AGOV-Account wird insbesondere im Bereich Straf- und Verwaltungsrecht begrüsst. Zu betonen ist, dass die Privatadresse im AGOV-Account nicht aktualisiert wird. Die Richtigkeit der Privatadresse beruht auf der Selbstdeklaration der Nutzerin oder des Nutzers. Sie wird anlässlich der Identifikation nicht geprüft, weshalb sie nicht verlässlich ist. Auch aus Sicht des Datenschutzes ist die Speicherung der Privatadresse in den Benutzerprofilen als kritisch zu betrachten. In den Profilen der natürlichen Personen sollte daher auf die Erhebung von Postadressen **verzichtet werden**.

Abs. 3 Bst. b

Unternehmen haben verschiedene Strukturen und verschiedene Niederlassungen, weshalb das verwendete digitale Profil nicht mit der Postadresse übereinstimmen muss. Die Postadresse bringt beim digitalen Zustellen daher keinen nennenswerten Mehrwert. **Auch bei Organisationen soll daher auf die Postadresse verzichtet werden.**

Absatz 3 sollte daher wie folgt lauten:

[3] *Die Profile der übrigen Benutzerinnen und Benutzer müssen mindestens folgende Angaben enthalten:*

a. bei natürlichen Personen: Vorname, Name, Geburtsdatum ~~sowie Postadresse~~;

b. bei Organisationen: Name oder Firma ~~und Postadresse~~.

Abs. 4

Der Sinn von Absatz 4 ist nicht verständlich. Es ist unklar, ob sich die Pflicht zur elektronischen Übermittlung auf die natürliche Person oder die Organisation, für welche die natürliche Person tätig ist, Bezug nimmt. Letzteres dürfte der Fall sein. Die Formulierung von Absatz 4 ist dementsprechend zu präzisieren.

Im erläuternden Bericht wird die verantwortliche Person einer Organisation erwähnt. Es ist wünschenswert, dass die Rolle der verantwortlichen Person in Bezug auf die zentrale Plattform in der Verordnung geklärt wird.

Art. 10 Schnittstelle

Dieser Artikel erlaubt den Nutzenden der Plattformen, ihre Systeme via eine Schnittstelle mit der Plattform zu verbinden und ihre Mitarbeitenden mit Vertretungsrechten auszustatten. Dies geschieht über einen technischen Benutzer, der ein digitales Passwort (Token) erhält. Die vorgeschlagene Regelung wird daher begrüsst.

Art. 11 Bestätigung und Entzug der Berechtigungen

Die vorgeschlagene Regelung in Absatz 1 wird begrüsst. Jedoch sollte in der französischen Version wohl eher von *Confirmation* als von *Attribution* gesprochen werden.

Die vorgeschlagenen Variante in Absatz 2 wird begrüsst.

5. Abschnitt: Datenschutz, Datensicherheit und Virenprüfung

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Problemstellung

Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein «Briefkasten» und keine Langzeitablage sein soll. Bei den Quittungen scheint es dagegen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Natürlich müssen die Behörden darum besorgt sein, die Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch aufgrund der Funktionsweise der zentralen Plattform – etwa im Fall von Zustellungen – dazu kommen, dass das Herunterladen der Quittungen unterbleibt. Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von der Plattform selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen.

Quittungen können Personendaten enthalten (so etwa die Namen von Verfahrensbeteiligten), was diese im Kontext von Justizverfahren unter Umständen zu besonders schützenswerten Personendaten macht. Jedoch sind diese Daten, wie auch die weitaus sensibleren Aktenstücke selbst, auf der Plattform verschlüsselt gespeichert. Hinzu kommt, dass es sich bei Quittungen um sehr kleine Datenmengen handelt, die keinen hohen zusätzlichen Speicherbedarf verursachen, selbst wenn sie lange auf der Plattform verfügbar bleiben müssen.

Lösungsansatz

In Anlehnung an die Zeitspanne von drei Jahren, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind, wird vorgeschlagen, Artikel 12 wie folgt zu ändern, respektive zu ergänzen:

> *Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen*
>
> *[1] Die auf einer Plattform gespeicherten Dokumente ~~und Quittungen~~ werden sechs Monate nach der Entgegennahme ~~beziehungsweise nach der Erstellung~~ automatisch vernichtet.*
>
> *[2] Stehen Dokumente zur Akteneinsicht zur Verfügung, so bestimmt die verfahrensleitende Behörde, wie lange die Dokumente auf der Plattform abrufbar sind. Nach Ablauf der Frist werden die Dokumente automatisch ~~vernichtet~~ gelöscht.*
>
> *[3] Quittungen werden drei Jahre nach ihrer Erstellung automatisch gelöscht.*

Abs. 2

Die vorgeschlagene Lösung wird begrüsst. Eine Verlängerung der Frist muss in der Verordnung nicht vorgesehen werden, da die Behörde eine zweite Akteneinsicht mit denselben Akten anordnen kann.

Art. 13 Datensicherheit

Die vorgeschlagene Bestimmung verweist auf den 3. Abschnitt, die Angabe des relevanten Kapitels (2.?) fehlt und sollte ergänzt werden.

Art. 14 Virenprüfung

Bei der vorgesehenen Prüfung auf Schadsoftware sind aus technischer Sicht drei Fälle zu unterscheiden:

1. Vollständige Prüfung der übermittelten Dateien: Die Maximalgrösse der einzelnen Dateien darf eine festgelegte Obergrenze nicht überschreiten, da die Prüfsoftware sonst ihr Limit (Speicherplatz usw.) erreichen, die Prüfung abbrechen und der Prüfvorgang so viel Zeit in Anspruch nehmen könnte, dass die Einhaltung von Fristen, besonders bei einer zeitlich knappen Eingabe, gefährdet wäre.

2. Eingeschränkte Prüfung grosser Dateien: Eine Datei, welche die festgelegte Obergrenze überschreitet, wird zum Zweck der Schadsoftware-Prüfung in handhabbare Blöcke zerlegt, die dann einzeln auf Schadsoftware geprüft werden. Dieses Verfahren ist jedoch weniger zuverlässig als die vollständige Prüfung der übermittelten Dateien. Schadsoftware, die durch die Aufteilung in prüfbare Blöcke auf zwei aufeinanderfolgende Blöcke verteilt wird, wird unter Umständen nicht mehr als Schadsoftware erkannt. Dies muss den Nutzerinnen und Nutzern der Plattform verständlich angezeigt werden. Insbesondere ist dem Empfänger klar zu signalisieren, dass er **eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten nach dem Herunterladen der Datei vornehmen muss.**

3. Keine Virenprüfung: Die zentrale Plattform kann die Virenprüfung nicht durchführen oder sie verzichtet auf Ersuchen der Benutzerin oder des Benutzers darauf.

Während der Pilotierung der zentralen Plattform hat sich gezeigt, dass die ergriffenen Schutzmassnahmen unter Umständen zu strikt sind und Dokumente aus verschiedenen Gründen zurückgewiesen wurden. Folgende Ursachen wurden während der Pilotierung identifiziert (nicht abschliessend):

- Übermittlung von passwortgeschützten oder end-2-end verschlüsselten Dateien zwischen bestimmten Behörden. Diese Dateien können prinzipiell nicht auf Schadsoftware geprüft werden, da sie verschlüsselt sind.
- Übermittlung von Dateiformaten mit Makros oder anderem ausführbaren Code: Diese enthalten zwar keine Viren im klassischen Sinne, bieten jedoch zahlreiche Angriffsmöglichkeiten für Cyberkriminelle. Aus diesem Grund werden ausführbare Dateiformate durch die Pilotplattform abgewiesen.
- Übermittlung von elektronischen Beweismitteln aus beschlagnahmten Geräten, im Original oder nach Aufbereitung durch die IT-Forensik, zum Beispiel im Rahmen der Akteneinsicht.
- Durch die ergriffenen Schutzmassnahmen werden Dateien fälschlicherweise zurückgewiesen, obwohl die Dateien von den sendenden Behörden bereinigt worden sind (sogenannte False-Positive).

In der Pilotierung wurde mehrfach gefordert, dass auch kritische Dateien übermittelt werden können, beispielsweise in einem digitalen Container. Die Behörden sollen dafür nicht auf alternative, unsichere Übermittlungswege ausweichen müssen (E-Mail, Cloud, UBS-Sticks, etc.). Die Ablage und Abholung dieser Dateien und die Prüfungen auf Schadsoftware obliegen in diesen Fällen den Nutzerinnen und Nutzern der Plattform. Wollen Sender und Empfänger auf Schutzmassnahmen verzichten, reduzieren sie die Funktion der Plattform auf die reine Übermittlung von Daten und sind selbst für den korrekten Umgang mit den Dateien verantwortlich. Dies bedingt eine ausdrückliche Absprache zwischen den Beteiligten. **Dies bedeutet auch, dass Nutzerinnen und Nutzer eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten jeweils vor und nach Übermittlung durch die zentrale Plattform vornehmen müssen.** Die Plattform muss den Empfänger zudem darauf hinweisen, dass die in einem Container übermittelten Dateien keiner Virenprüfung unterzogen worden sind.

Abs. 1

Die Festlegung der (Maximal-)Grösse von prüfbaren Blöcken grösserer Dateien sollte nicht öffentlich kommuniziert werden. Diese Information ist für die Nutzerinnen und Nutzer der Plattform irrelevant. Sie eröffnet potenziellen Angreifern die Möglichkeit, ihre Schadsoftware in einer verseuchten Datei so anzuordnen, dass der Schadcode bei der Aufspaltung in mehrere Blöcke in zwei aufeinanderfolgenden Blöcken liegt und nicht zuverlässig als schädlich erkannt werden kann. Zudem wird es stark von der für die Aufspaltung und Prüfung zuständigen Software abhängen, wie gross diese prüfbaren Blöcke zu gestalten sind. Diese Grenze wird sich aufgrund von Betriebserfahrung und Verbesserungen in der Hard- und Software dynamisch verändern und sollte einfach anpassbar sein.

Absatz 1 sollte zusammengefasst wie folgt lauten:

> [1] *Die Plattformen ~~müssen bei bis zu 64 Megabyte grossen Dateien~~ führen eine Virenprüfung durch~~führen~~.*

Abs. 2

Der Grenzwert für eine vollständige Prüfung auf Schadsoftware von derzeit 64 MB kann (und sollte) basierend auf den technischen Möglichkeiten und der wachsenden Betriebserfahrung durch die Betreiber der Plattformen erhöht werden können. **Absatz 2 ist daher zu streichen**.

> *~~[2] Dokumente ab 64 Megabyte können sie in 64 Megabyte grosse Dokumente aufteilen und diese einer Virenprüfung unterziehen.~~*

Abs. 4

Eine klare Kennzeichnung ist auch dann essenziell, wenn die Virenprüfung nur eingeschränkt stattgefunden hat. Absatz 4 ist dementsprechend zu ergänzen. Unklar ist allerdings, wie die Ergebnisse der Virenprüfung den Nutzenden mitgeteilt werden. Die Mitteilung sollte technisch einfach und inhaltlich leicht verständlich erfolgen können.

Absatz 4 sollte wie folgt lauten:

> *[4] Dokumente, bei denen ~~eine Virenprüfung nach Absatz 2~~ keine oder eine eingeschränkte Virenprüfung durchgeführt wurde, müssen entsprechend gekennzeichnet werden.*

Abs. 5

Bei der Information der Plattformen an die Absenderin oder den Absender, dass ein Dokument nicht übermittelt werden konnte, handelt es sich klarerweise nicht um eine Quittung, da eben kein Dokument übermittelt worden ist (vgl. Ausführungen zu Art. 5 Abs. 2 Bst. d Ziff. 2 oben).

6. Abschnitt: Gebühr für die Nutzung der zentralen Plattform

Basis für die Berechnung der Gebühr bilden die Artikel 6 und 32 des BEKJ. Die Kosten der zentralen Plattform werden auf die nutzenden Kantone aufgeteilt. Für die Mitglieder der Körperschaft berechnet sich der Gebührenanteil anhand der ständigen Wohnbevölkerung. Mit Nichtmitgliedern schliesst die Körperschaft eine Vereinbarung gemäss Artikel 6 BEKJ ab. Die vereinbarte Vergütung soll sämtliche Kosten decken (inklusive Investitionskosten, Botschaft BEKJ, BBl 2023 679, S. 22), welche das Nichtmitglied verursacht. Die Kosten für Nichtmitglieder werden daher in der Regel höher ausfallen als jene der Mitglieder.

Art. 15 Berechnung der Gebühr

Die deutsche und die französische Fassung wurden verglichen und vereinheitlicht; dies betrifft auch die konsistente Terminologie für denselben Sachverhalt. Für mehr Klarheit wurde der Absatz 1 in (neu) zwei Absätze aufgeteilt.

Die Dreijahresfinanzplanung als Referenz für die Festlegung des Gesamtbetrags für drei Jahre wird begrüsst. Der Ansatz liefert eine vorausschauende und realistische Grundlage für die jährlich gemäss Verteilschlüssel in Artikel 16 festzulegende Gebühr. Das ergänzende Korrektiv gemäss Absatz 4 stellt die notwendige Anpassungsfähigkeit sicher.

Folgender Text wird vorgeschlagen:

> *[1] ~~Die Gesamthöhe~~ Der Gesamtbetrag der jährlich von den Mitgliedern der öffentlich-rechtlichen Körperschaft zu entrichtenden Gebühr ~~für die Nutzung der zentralen Plattform~~ muss die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform decken und die Bildung einer Reserve für die Sicherstellung der Liquidität der öffentlich-rechtlichen Körperschaft in der Höhe von 10 Prozent der jährlichen Betriebskosten ~~ermöglichen~~ gewährleisten.*
>
> *[Anpassung und neuer Absatz 2]*
>
> *[2] ~~Die Einnahmen aus Leistungsbezügen der~~ Beiträge von Kantonen, die nicht Mitglied der öffentlich-rechtlichen Körperschaft sind, werden vom Gesamtbetrag der jährlichen Gebühr abgezogen.*

[3] Das EJPD legt ~~die jährliche~~ den Gesamtbetrag der jährlichen Gebühr ~~aufgrund~~ für jeweils drei Jahre im Voraus auf der Grundlage der Finanzplanung der öffentlich-rechtlichen Körperschaft fest.

[4] Das EJPD kann die Gebühr während der Periode nach Absatz 3 ~~2~~ anpassen, wenn die eingenommenen Beiträge nach Absatz 1 und 2 ~~diese Gebühr~~ die Betriebs- und Weiterentwicklungskosten nicht ~~deckt~~ decken oder die Reserve die Limite nach Absatz 1 überschreitet.

Art. 16 Aufteilung der Gebühr

Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 Prozent wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die Aufteilung der Gebühr sollte Gegenstand der Prüfung sein.

Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen. Anhand dieser verbindlichen Angaben legt das EJPD den jährlichen Gebührenbeitrag fest; es berücksichtig dabei die in Artikel 15 Absatz 4 definierten Schwellenwerte und den allfälligen Beitritt eines Nichtmitgliedes zur Körperschaft justitia.swiss nach deren Gründung (vgl. Art. 19 Vereinbarung justitia.swiss sowie erläuternder Bericht zur Vereinbarung justitia.swiss, S. 17).

Vorgeschlagen wird folgender Wortlaut:

[1] Die Gesamthöhe der Gebühr wird wie folgt auf den Bund und die Kantone, die Mitglied der öffentlich-rechtlichen Körperschaft sind, aufgeteilt:

a. Bundesverwaltung und Bundesanwaltschaft (BA): 5 Prozent;

b. Eidgenössische Gerichte: 5 Prozent;

c. Kantone: 90 Prozent.

[2] Der Anteil der Kantone wird ~~gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt~~ unter den Kantonen, die Mitglieder der öffentlich-rechtlichen Körperschaft sind, proportional zu deren ständigen Wohnbevölkerung am 1. Januar des Vorvorjahres, für das die Gebühr fällig wird, verteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen ~~im Zeitpunkt der Festlegung nach Artikel 15~~.

[3] Das EJPD legt jährlich die Verteilung der Gebühr auf die Kantone fest.

Art. 17 Gebührenanteil der Bundesverwaltung und der Bundesanwaltschaft

Keine Bemerkungen.

Art. 18 Gebührenanteil der eidgenössischen Gerichte

Keine Bemerkungen.

Art. 19 Fälligkeit

Die Verordnung lässt die weiteren Modalitäten der Erfüllung offen. Es ist anzunehmen, dass die Regeln des Obligationenrechts sinngemäss zur Anwendung kommen. Vorgeschlagen wird daher folgender Wortlaut der Bestimmung:

> *[1] Die jährliche Gebühr der Mitglieder der öffentlich-rechtlichen Körperschaft ist ~~sind~~ im Voraus zu entrichten und am 1. Januar fällig.*
>
> *[2] Die Gebühr für ~~das erste Betriebsjahr der öffentlich-rechtlichen Körperschaft ist an dem Tag fällig, an dem diese Verordnung in Kraft tritt~~ die Nutzung der zentralen Plattform ist erstmals am Tag des Inkrafttretens dieser Verordnung fällig.*
>
> *[3] Die Bestimmungen des Obligationenrechts zum Schuldnerverzug finden sinngemäss Anwendung.*

Art. 20 Rechnungsstelle der Kantone

Keine Bemerkungen.

Art. 21 Evaluation der Gebührenregelung

Die Überprüfung der Berechnungsweise und der Aufteilung der Gebühr wird begrüsst.

2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten

Art. 22 Digitalisierung von physischen Dokumenten

Diese Bestimmung betrifft alle Behörden, welche Verfahren leiten und deren Verfahrensrecht das BEKJ für anwendbar erklärt (Art. 2 BEKJ). Für die Kantone stehen daher die Zivilprozessordnung, das Opferhilfegesetz und die Strafprozessordnung im Vordergrund.

Das in Absatz 2 vorgeschriebene Format PDF/A erleichtert die Archivierung der Justizakten. Unklar ist, ob dieses Format durch die sehr unterschiedlichen kantonalen Justizapplikationen leicht verarbeitet werden kann.

Absatz 3 sieht die Texterkennung vor. Diese scheint in vielen Fällen sinnvoll und erleichtert die Bearbeitung der Dokumente. Bei fremdsprachigen Texten kann das Ergebnis der Texterkennung gemäss aktuellem Stand der Technik jedoch unbefriedigend oder fehlerhaft sein. Die Auflösung von 300 DPI scheint sinnvoll zu sein. Anzumerken ist, dass die Dateigrösse bei der Auflösung von 300 DPI viermal grösser ist als bei der Auflösung von 150 DPI.

Art. 22*a* (neu) Rücksendung von physischen Dokumenten

Problemstellung

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7) wird dargelegt, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Artikel 30 BEKJ in die vorliegende Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe.

Diese Feststellung bezieht sich auf die Auslegung des in Artikel 30 BEKJ enthaltenen Begriffs der «Dokumente», der im Gesetz weder weiter nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird. Eine differenzierende Betrachtung ist nach hier vertretener Auffassung aber erforderlich, um mit einer lückenhaften Verordnung zum BEKJ keine Probleme zu schaffen, die es in der analogen Welt noch gar nicht gibt. Damit ist auch gesagt, dass die anwendbaren Prozessgesetze nach hier vertretener Meinung durchaus Raum für eine Auslegung der Bestimmungen des BEKJ im Sinne ihrer gesetzgeberischen Zielsetzung lassen.

Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende

von Anzeigen in Papierform eingehen, weil derlei Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es in der analogen Welt noch gar nicht gab. Dies kann nicht der Willen des Gesetzgebers gewesen sein.

Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft, die im Schriftstück enthalten ist. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden überwiegend weggeworfen werden, sobald sie wieder bei ihren ursprünglichen Absenderinnen und Absendern eingetroffen sind.

Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, könnte mit den zurückgeschickten Dokumenten nicht Beweis geführt werden, weil sich nicht feststellen liesse, ob es auch diese Papiere waren, die gegenüber der Behörde eingereicht worden waren.

Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Artikel 30 Absatz 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Der Botschaft zum BEKJ ist zu entnehmen, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen (Botschaft BEKJ, BBl 2023 679, S. 36). Damit ist auch gesagt, dass die Rücksendepflicht von Urkunden, an deren Wiedererhalt die Absenderinnen und Absender ein Interesse haben, vorliegend nicht in Frage gestellt wird.

Hingegen braucht nicht weiter ausgeführt werden, dass durch die Auslegung des BEKJ im Sinne eines neu geschaffenen, replizierenden Postverkehrs in Papierform ein enormer Mehraufwand durch Porti und Arbeitsaufwand geschaffen wird. Eine Gesetzesauslegung, die letztlich dazu führt, dass tausende von Altpapierbündeln mit Porto versehen werden müssen, kann nicht von der gesetzgeberischen Absicht getragen sein.

Lösungsansatz

Aus den oben genannten Gründen wird vorliegend vorgeschlagen, einen neuen Artikel 22a einzufügen. Die gewählte Formulierung stellt klar, dass Dokumente, die gemäss Artikel 30 Absatz 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Artikel 30 BEKJ in die Verordnung zu schreiben. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen:

> *2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten*
>
> […]
>
> *Art. 22a Rücksendung von physischen Dokumenten*
>
> *Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.*

Art. 22*b* (neu) **Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten**

Problemstellung: Wie erreicht man Personen, welche nicht auf der Plattform erreichbar sind?

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7 f.) wird ausgeführt, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Artikel 353 Absatz 1 Buchstabe k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: «Der Strafbefehl enthält: (…) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.» Artikel 238 Buchstabe h nZPO enthält eine ähnliche Regelung für zivilgerichtliche Entscheide.

Artikel 22 konkretisiert Artikel 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ zwar die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird.

Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von zehn bis zwanzig Prozent der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Zwar liegt dem BEKJ als Regulierungsgrundsatz die Idee zugrunde, dass Privatpersonen nicht zur elektronischen Kommunikation mit den Behörden gezwungen werden sollen und an dieser Grundlage soll vorliegend deshalb auch nicht gerüttelt werden. Hingegen kann es nicht richtig sein, das Unterschriftserfordernis derart restriktiv auszulegen, dass jeglichem Fortschritt ein Riegel vorgeschoben wird.

Artikel 22 Absatz 2 BEKJ ist zu entnehmen, dass künftig mittels eines geregelten elektronischen Siegels sichergestellt werden soll, dass ein elektronisch erstelltes Dokument tatsächlich von der zuständigen Behörde stammt, die sich etwa aus dem Briefkopf o.ä. ergibt. Zu diesem Artikel ist der Botschaft zum BEKJ zu entnehmen: «Das Unterschriftserfordernis stellt bei der Digitalisierung oft ein Hindernis dar. Anstelle der Unterschrift sieht das Gesetz die Authentifizierung mit Hilfe eines anerkannten elektronischen Identitätsnachweises sowie dem Anbringen eines geregelten elektronischen Siegels vor.» (Botschaft BEKJ, BBl 2023 679 S. 30). Damit ist gesagt, dass das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift ersetzt. Für einen Rückgriff auf Artikel 14 OR bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel (zum Schutzniveau vgl. Botschaft BEKJ, a.a.O.).

Lösungsansatz

Zwar ist dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens insoweit beizupflichten, dass den massgeblichen Verfahrensgesetzen zu entnehmen ist, dass etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Nach hier vertretener Auffassung lässt diese Formulierung aber durchaus eine Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes zu.

Bereits heute ist es absolut gängige Praxis bei den Zivilgerichten und den Strafbehörden, das Original der Endentscheide zu den Akten der Behörde zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen. Wie schon weiter oben zur Bestimmung über den Rückversand eingesandter Papierdokumente

ausgeführt, wird nun durch den Verzicht auf eine reduzierende Auslegung eine neue Pflicht in der analogen Welt geschaffen. Wird dem erläuternden Bericht gefolgt, soll es plötzlich eine Pflicht zum Versand von Papieroriginalen geben. Damit wird der Versand von Papieroriginalen in der digitalen Welt exponentiell vervielfacht. Das kann nicht die Idee der Gesetzgebung gewesen sein.

Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Einer Papierkopie des elektronischen Originals kommt exakt derselbe Informationsgehalt zu wie ein Entscheid, der eine handschriftliche Signatur trägt. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann.

Die vorgeschlagene Lösung hätte den Vorteil, dass in einem Verfahren keine zwei Originale desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids (ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG stellt für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Aus den in Ziffer 3.1 genannten Gründen wird deshalb vorgeschlagen, einen neuen Artikel 22b einzufügen:

> ***Art. 22b*** *Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten*
>
> *Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.*

Sollte an der viel zu engen Auslegung des BEKJ festgehalten werden, die im erläuternden Bericht skizziert ist, wäre zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen, um dem in den Verfahrensgesetzen verwendeten Begriff der «Unterschrift» genüge zu tun, obwohl diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung durch das Behördensiegel ersetzt wurde.

3. Kapitel: Elektronische Übermittlung ausserhalb einer Plattform nach dem BEKJ

1. Abschnitt: Verwendung von anderen Lösungen zur Übermittlung von Dokumenten

Art. 23 Eignungsvoraussetzungen

Diese Bestimmung konkretisiert die Artikel 128b Absatz 2 der Zivilprozessordnung, Artikel 103b Absatz 2 der Strafprozessordnung und Artikel 8c Absatz 2 des Opferhilfegesetzes vom 23. März 2007. Die Kantone gehen davon aus, dass sich diese Bestimmung an die Kommunikation zwischen Strafbehörden innerhalb der Strafprozesskette richtet, bei der Akten beispielsweise bei einem Weiterzug an die übergeordnete Instanz weitergeben müssen, wo andere Behörden mit bestimmten Verfahrenshandlungen beauftragt werden (Bsp. Ermittlungsauftrag von Staatsanwaltschaft an die Kriminalpolizei) oder bei der Übermittlung von Ergebnissen von Untersuchungshandlungen, welche die Polizei an die Staatsanwaltschaft übermittelt.

Ein zweites Anwendungsfeld ist die Zivilprozesskette, beispielsweise wenn ein Zivilgericht das Betreibungs-, das Konkursamt oder das Handelsregisteramt anweist, eine bestimmte Handlung vorzunehmen oder, wenn das erstinstanzliche Gerichte seine Akten aufgrund des Weiterzugs an die kantonale Rechtsmittelinstanz weitergibt.

Die physische Weitergabe der Akten zwischen Strafbehörden erfolgt aktuell noch oft auf dem Postweg, mit interner Post oder dem Kurierdienst. Die Beauftragung der Polizei für Untersuchungshandlung ergeht in der Regel schriftlich, jedoch werden weder genauer Zeitpunkt noch der Empfang gesondert festgehalten.

Die vorgeschlagenen Ausführungsbestimmungen orientieren sich stark an der technischen Lösung der zentralen Plattform. Bei der elektronischen Weitergabe innerhalb des Kantons (ZPO) oder unter Strafbehörden (StPO) sollten jedoch andere Anforderungen gelten als bei der Kommunikation über die zentrale Plattform.

Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank erfolgen. Dafür braucht es nach Einschätzung der Kantone keine Quittung. Die Protokollierung in den Logfiles des kantonalen IT-Systems genügen. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem mehrmaligen Versand von Dokumenten über eine externe Plattform klar vorzuziehen.

Artikel 23 sollte so ergänzt werden, damit die elektronische Weitergabe von Dokumenten durch die Mutation von Zugriffsrechten auf eine gemeinsame Datenbank zulässig ist. Die Nachvollziehbarkeit der Zeitpunkte der Übermittlung oder der Mutation von Zugriffsrechten muss gewährleistet sein. Die Anforderungen von ZPO und StPO gehen nicht so weit, dass in der digitalen Umsetzung ein synchronisierter Zeitstempel wie in Buchstabe b notwendig wäre. Deshalb ist auf dieses Kriterium zu verzichten.

Art. 24 Elektronische Übermittlung unter Behörden

Nach Einschätzung der Kantone ist die Sachüberschrift zu weit gefasst und daher irreführend. Es handelt sich stets um die Kommunikation von und zu Strafbehörden oder Zivilgerichten im Rahmen von Verfahren nach StPO oder ZPO. Gleichzeitig erscheint es erforderlich, den Begriff der übrigen Behörden, also jene, die unter das Obligatorium fallen, mit den Strafbehörden elektronisch kommunizieren zu müssen, zu definieren (vgl. Bemerkungen zu Art. 6 oben). Insbesondere mit Blick auf öffentlich-rechtliche Körperschaften, die nicht hoheitlich handeln, besteht insoweit Unklarheit.

Diese Bestimmung konkretisiert die Ausnahmen von Artikel 128c Absatz 2 der Zivilprozessordnung, Artikel 103c Absatz 2 der Strafprozessordnung und Artikel 8d Absatz 2 des Opferhilfegesetzes. Diese Ausnahmen sind dort sinnvoll, wo in Zivil- oder Strafverfahren eine grosse Anzahl von Kommunikationen mit Behörden anfallen, die nicht Teil der Straf- oder Zivilprozesskette sind und wo eine direkte Kommunikation, z.B. über eine Schnittstelle, etwa zur Weitergabe von Metadaten oder aus Kostengründen dem Rechtsverkehr über die Plattform vorzuziehen ist. Zu denken ist im Strafprozess etwa an Steuer- oder Migrationsbehörden oder auch an grosse Verkehrsbetriebe oder rechtsmedizinische Institute, die auch unter den Behördenbegriff fallen dürften. Ebenso bestimmte Behörden des Bundes wie das BAZG.

Die Voraussetzungen sollten sich an Artikel 23 orientieren und nicht darüber hinausgehen. Es ist jedenfalls nicht ersichtlich, weshalb Artikel 24 strengere Anforderungen vorsieht, da Artikel 103c Absatz 2 der Strafprozessordnung – anders als Art. 103b Absatz 2 mit der Feststellung der Zeitpunkte der Übermittlung und dem Schutz der Akte vor Veränderung und unberechtigter Kenntnisnahme - überhaupt keine Anforderungen an die Dokumentation einer Übermittlung stellt.

2. Abschnitt: Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Art. 25 Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Keine Bemerkungen.

3. Abschnitt: Elektronische Bestätigung von Protokollen im Straf- und Militärstrafprozess

Art. 26 Elektronische Bestätigung von Protokollen im Straf- und Militärstrafprozess

Keine Bemerkungen.

4. Kapitel: Schlussbestimmungen

Art. 27 Aufhebung und Änderung anderer Erlasse

Keine Bemerkungen.

Art. 28 Inkrafttreten

Die Finanzierung des Projekts Justitia 4.0, welches die zentrale Plattform im Auftrag der Kantone, des Bundes und der Justizbehörden aufbaut, ist bis Ende Jahr 2027 gesichert. Die Finanzierung von Betrieb und Weiterentwicklung der zentralen Plattform muss daher spätestens ab Anfang 2028 über Gebühren erfolgen. Die Verordnung muss gleichzeitig mit dem abschliessendem Inkrafttreten des BEKJ in Kraft gesetzt werden.

Aufhebung und Änderung anderer Erlasse

Aufhebung VeÜ-VwV

Keine Bemerkungen.

Aufhebung VeÜ-ZSSV

Durch die Aufhebung der Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren können IncaMail und PrivaSphere in Verfahren, die nach dem Inkrafttreten der Verordnung begonnen haben, nicht mehr genutzt werden. Es ist daher an den Kantonen, für Verwaltungsverfahren, welche nicht über die Plattform justitia.swiss abgewickelt werden können, geeignete Kanäle auszuwählen und bereit zu stellen.

Art. 14a VZertES Vom Validator zu prüfende Signaturen und Siegel

Keine Bemerkungen.

Art. 14b VZertES Anbringen und validieren von elektronischer Signatur und Siegel

Keine Bemerkungen.

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
E-Mail: staatskanzlei@bs.ch
www.bs.ch/regierungsrat

Eidgenössisches Justiz- und Polizeidepartement (EJPD)

Per E-Mail an:
cornelia.perler@bj.admin.ch

Basel, 2. Juni 2026

Regierungsratsbeschluss vom 2. Juni 2026

Erlass der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Vernehmlassung; Stellungnahme des Kantons Basel-Stadt

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie uns die Vernehmlassungsunterlagen zum Erlass der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) zukommen lassen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und lassen Ihnen nachstehend unsere Anträge und Bemerkungen zukommen.

1. Grundsätzliche Einschätzung

Der Regierungsrat begrüsst im Grundsatz den Vorentwurf der VEKJ und die darin enthaltene Festlegung bzw. Präzisierung der Anforderungen an den elektronischen Rechtsverkehr im Anwendungsbereich des Bundesgesetzes über die Plattformen für die elektronische Kommunikation (BEKJ) vom 20. Dezember 2024, mit den Änderungsvorschlägen in der nachfolgenden Ziff. 2.

Als Herausforderung erachtet der Regierungsrat die Parallelität und das technische Zusammenspiel von aktuell sich entwickelnden Projekten im Justizbereich. Hier wäre zu befürworten, dass die verschiedenen Projekte bereits auf Bundesebene zu einem Minimum IT-architektonisch aufeinander abgestimmt werden. Ausserdem erachtet er als sinnvoll, wenn in der Verordnung selbst möglichst wenige technische Details (Dateiformat, Dateigrösse usw.) festlegt werden, da die Entwicklungen weiterhin dynamisch sind.

2. Anträge zu den einzelnen Änderungsvorschlägen

2.1 Artikel 2 (Anforderungen an die Plattformen)

2.1.1 Löschrecht und Nachweisbarkeit (Art. 2 Abs. 1 lit. d)

Die Bestimmung sieht vor, dass Benutzerinnen und Benutzer Dokumente und Quittungen in ihrem Profil jederzeit löschen können. Aus Sicht der Vollzugsbehörden wirft dies eine kritische Frage zur Beweissicherheit auf: Sofern eine Nutzerin bzw. ein Nutzer eine Abrufquittung löscht, muss sichergestellt sein, dass die zustellende Dienststelle dennoch jederzeit einen revisionssicheren Nachweis über den erfolgten Abruf (Zustellzeitpunkt) führen kann.

Antrag: Es ist in der Verordnung oder den Erläuterungen klarzustellen, dass das Löschrecht im Benutzerprofil die Pflicht der Plattform zur Aufbewahrung der Zustellnachweise (Audit Logs) für die Behörden (analog der 90-Tage-Frist in Art. 22 Abs. 5 BEKJ) nicht tangiert.

2.1.2 Delegationsnorm und Timeline (Art. 2 Abs. 2)

Die detaillierten funktionalen Anforderungen werden erst in einer Departementsverordnung des EJPD geregelt. Für die Planung kantonaler Umsetzungsprojekte ist die technische Spezifikation (APIs, Datenformate) aber von existenzieller Bedeutung.

Antrag: Wir bitten um eine zeitnahe Kommunikation der Roadmap für den Erlass dieser Departementsverordnung.

2.2 Artikel 4 (Format der Dokumente)

2.2.1 Begrifflichkeit (Art. 4 ff.)

Wie bereits das BEKJ verwendet der Vorentwurf in verschiedenen Artikeln den Begriff "Dokument" anstelle von «Datei». In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wurde dies damit begründet, dass der Begriff "Datei" für das Gesetz zu technisch sei.

Antrag: In diesem Sinne ist in der Verordnung der Begriff Datei – an Stelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

2.2.2 Normstufe (Art. 4 Abs. 3 und 4)

Die Nennung der Medienformate wird grundsätzlich begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen.

Die Liste der unterstützten Medienformate ist einem stetigen Wandel unterworfen. Es sind daher häufige Anpassungen zu erwarten. Zudem ist das reine Benennen von Formaten in der Verordnung nicht ausreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei dennoch verschlüsselten oder passwortgeschützten Elementen (z. B. Makros in einer Microsoft Excel-Datei, ZIP-Dateien mit teilweise verschlüsselten Dateien etc.). Dies ist in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung.

Antrag: In Art. 4 Abs. 3 und 4 ist anstelle der Aufzählung von Medienformaten auf eine separate Regelung (in einem Anhang oder einer Departementsverordnung) zu verweisen. Die separate Regelung hat zudem weitere technische Details zu enthalten (wie vorgängig ausgeführt).

2.2.3 Ergänzung der Aufzählung (Art. 4 Abs. 3)

Die Kantonspolizei Basel-Stadt verwendet Smartpolice für die Aufnahme und Ablage von fallbezogenen Mediendateien. Auch die im Smartpolice verwendeten Medienformate sollten deshalb durch die Plattform unterstützt werden.

Antrag: Sollte weiterhin eine Aufzählung der Medienformate in der Verordnung oder einer separaten Regelung geführt werden, sind die in Smartpolice verwendeten Formate zu ergänzen.

2.3 Artikel 5 (Quittungen)

Die Verordnung verlangt, dass Quittungen sowohl von Menschen als auch von Maschinen lesbar sein müssen. In der Verordnung sollte klargestellt werden, welche Formate hierfür vorgesehen sind. Während PDF/A für die menschliche Lesbarkeit gesetzt ist, kommen für die Maschinenlesbarkeit (automatisierte Verarbeitung in Fachanwendungen) primär XML oder JSON in Frage. Eine pauschale Implikation, dass PDF/A ausreichend «maschinenlesbar» sei, greift zu kurz. Aus redaktioneller Sicht ist zu bemerken, dass die Struktur der Absätze 3 bis 5 unnötig kompliziert erscheint.

Antrag: Der Wortlaut von Art. 5 Abs. 3 ist so zu vereinfachen, dass klar zwischen dem Darstellungskanal (Mensch/Auge) und dem Datenkanal (Maschine/Schnittstelle) unterschieden wird und die jeweils zwingenden Formate benennt werden.

2.4 Artikel 6 (Siegelung durch übermittelnde Behörde)

Hier besteht ein Widerspruch zum erläuternden Bericht: Art. 6 VEKJ sieht vor, dass bei der Übermittlung mehrerer Dokumente durch eine Behörde die Siegelung eines einzigen Dokuments ausreicht. Dies steht im direkten Widerspruch zum erläuternden Bericht (S. 18, 1. Absatz zu Art. 6), welcher festhält: «Bei Versand durch eine Behörde, muss sie alle Dokumente mit einem Siegel und einem Zeitstempel versehen.»

Antrag: Um Rechtsunsicherheit zu vermeiden, ist dieser Widerspruch aufzulösen. Dies erfolgt am besten durch eine Erleichterung im Verordnungstext (ein Siegel pro Sendung), sofern die Integrität der gesamten Sendung über die Quittung (Hashwerte) technisch gesichert bleibt.

2.5 Artikel 7 (Siegelung durch die Plattform)

Wenn die Plattform bei Eingaben von Privaten ein separates Dokument mit Siegel und Zeitstempel erstellt, stellt sich die Frage nach der Redundanz zur Eingangsquittung nach

Art. 5 Abs. 2 lit. d. Es stellt sich die Frage, ob das Siegeldokument hier eine zusätzliche Funktion übernimmt, oder ob Siegel und Hashwerte nicht integraler Bestandteil der Quittung selbst sein sollten. Eine Zersplitterung der Nachweisdokumente erschwert die Aktenführung.

Antrag: Der Wortlaut sollte präzisiert werden, um klarzustellen, dass bei der Verwendung bereits bestehender Siegel oder Signaturen stets ein qualifizierter elektronischer Zeitstempel zwingend ist. Dies muss sowohl für das Siegel als auch für die qualifizierte Signatur gelten, um die Fristwahrung lückenlos nachzuweisen.

2.6 Artikel 8 (Authentifizierung der Benutzerinnen und Benutzer)

Die Authentifizierung über AGOV gemäss Abs. 1 oder Alternativen mit mindestens so hoher Authentifizierungsqualität gemäss Abs. 2 ist sinnvoll und zielführend. Als alternative Authentifizierungsdienste für Mitglieder von Behörden gemäss Abs. 3 sollten die Zertifikate des EJPD SSO Portals (Login auf die zentrale Plattform via EJPD-Portal) ebenfalls zugelassen werden.

Antrag: Die Zertifikate des EJPD SSO Portals (Login auf die zentrale Plattform via EJPD-Portal) sind als «andere Authentifizierungsdienste» im Sinne von Art. 8 Abs. 3 in Erwägung zu ziehen.

2.7 Artikel 22a (neu: Rücksendung von physischen Dokumenten)

In Ziffer 2.6 des erläuternden Berichts wird dargelegt, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Art. 30 BEKJ in die VEKJ aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe. Diese Feststellung bezieht sich auf die Auslegung des in Art. 30 BEKJ enthaltenen Begriffs der «Dokumente», der im Gesetz weder weiter nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird. Eine differenzierende Betrachtung ist aber erforderlich, um mit einer lückenhaften Verordnung zum BEKJ keine Probleme zu schaffen, die es in der analogen Welt noch gar nicht gibt. Damit ist auch gesagt, dass die anwendbaren Prozessgesetze nach hier vertretener Meinung durchaus Raum für eine Auslegung der Bestimmungen des BEKJ im Sinne ihrer gesetzgeberischen Zielsetzung lassen.

Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen in Papierform eingehen, da solche Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es in der analogen Welt noch gar nicht gab. Dies kann nicht der Wille des Gesetzgebers gewesen sein.

Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft, die im Schriftstück enthalten ist. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden überwiegend weggeworfen, sobald sie wieder bei ihren ursprünglichen Absenderinnen und Absendern eingetroffen sind. Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, könnte mit den zurückgeschickten Dokumenten nicht Beweis geführt werden, weil sich nicht feststellen liesse, ob es auch diese Papiere waren, die gegenüber der Behörde eingereicht worden waren.

Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Art. 30 Abs. 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Der Botschaft zum BEKJ ist zu entnehmen, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen (Botschaft BEKJ, BBl 2023 679, S. 36). Damit ist auch gesagt, dass die Rücksendepflicht von Urkunden, an deren Wiedererhalt die Absenderinnen und Absender ein Interesse haben, vorliegend nicht in Frage gestellt wird.

Hingegen braucht nicht weiter ausgeführt werden, dass durch die Auslegung des BEKJ im Sinne eines neu geschaffenen, replizierenden Postverkehrs in Papierform ein enormer Mehraufwand durch Porti und Arbeitsaufwand geschaffen wird. Eine Gesetzesauslegung, die dazu führt, dass tausende von Altpapierbündeln mit Porto versehen werden müssen, kann nicht von der gesetzgeberischen Absicht getragen sein.

Antrag: Es sei ein neuer Art. 22a einzufügen, der klarstellt, dass Dokumente, die gemäss Art. 30 Abs. 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Art. 30 BEKJ in die Verordnung zu schreiben. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen.

2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten

[...]

Art. 22a Rücksendung von physischen Dokumenten

[1] Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.

2.8 Artikel 22b (neu: Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten)

In Ziffer 2.6 des erläuternden Berichts wird ausgeführt, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Art. 353 Abs. 1 Bst. k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: «Der Strafbefehl enthält: (...) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.» Art. 238 Bst. h nZPO enthält eine ähnliche Regelung für zivilgerichtliche Entscheide.

Art. 22 konkretisiert Art. 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ zwar die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird.

Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von zehn bis zwanzig Prozent der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Zwar liegt dem BEKJ als Regulierungsgrundsatz die Idee zugrunde, dass Privatpersonen nicht zur elektronischen Kommunikation mit den Behörden gezwungen werden sollen und an dieser Grundlage soll vorliegend deshalb auch nicht gerüttelt werden. Hingegen kann es nicht richtig sein, das Unterschriftserfordernis derart restriktiv auszulegen, dass jeglichem Fortschritt ein Riegel vorgeschoben wird.

Art. 22 Abs. 2 BEKJ ist zu entnehmen, dass künftig mittels eines geregelten elektronischen Siegels sichergestellt werden soll, dass ein elektronisch erstelltes Dokument tatsächlich von der zuständigen Behörde stammt, die sich etwa aus dem Briefkopf o.ä. ergibt. Damit ersetzt das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift. Für einen Rückgriff auf Artikel 14 OR bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel.

Zwar ist dem erläuternden Bericht insoweit beizupflichten, dass den massgeblichen Verfahrensgesetzen zu entnehmen ist, dass etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Nach hier vertretener Auffassung lässt diese Formulierung aber durchaus eine Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes zu. Bereits heute ist es absolut gängige Praxis bei den Zivilgerichten und den Strafbehörden, das Original der Endentscheide zu den Akten der Behörde zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen. Wie schon weiter oben zur Bestimmung über den Rückversand eingesandter Papierdokumente ausgeführt, wird nun durch den Verzicht auf eine reduzierende Auslegung eine neue Pflicht in der analogen Welt geschaffen. Wird dem erläuternden Bericht gefolgt, soll es plötzlich eine Pflicht zum Versand von Papieroriginalen geben. Damit wird der Versand von Papieroriginalen in der digitalen Welt exponentiell vervielfacht. Das kann nicht die Idee der Gesetzgebung gewesen sein.

Antrag: Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Einer Papierkopie des elektronischen Originals kommt exakt derselbe Informationsgehalt zu wie ein Entscheid, der eine handschriftliche Signatur trägt. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann.

Die vorgeschlagene Lösung hätte den Vorteil, dass in einem Verfahren keine zwei Originale desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids (ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG stellt für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Aus den genannten Gründen sei deshalb ein neuer Artikel 22b einzufügen:

> **Art. 22b** Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten
>
> [1] Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen.
>
> [2] Soweit diese Dokumente Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals.
>
> [3] Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Ihnen gerne das Generalsekretariat des Justiz- und Sicherheitsdepartements, Frau Stephanie Matter, stephanie.matter@jsd.bs.ch, Tel. 061 267 77 74, zur Verfügung.

Freundliche Grüsse
Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Conradin Cramer
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail
(cornelia.perler@bj.admin.ch) (Im PDF- und im Word-Format)

RRB Nr.:	660/2026	17. Juni 2026
Direktion:	Direktion für Inneres und Justiz	
Klassifizierung:	Nicht klassifiziert	

Vernehmlassung des Bundes: Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)
Stellungnahme des Kantons Bern

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur erwähnten Vorlage Stellung nehmen zu können. Der Regierungsrat möchte dazu die nachfolgenden Bemerkungen anbringen.

1. Grundsätzliches

Wir stimmen dem Verordnungsentwurf zu unter Vorbehalt der nachfolgenden Anträge und Bemerkungen.

Einleitend halten wir sodann Folgendes fest:

Die VEKJ wird erhebliche Auswirkungen auf die Arbeit der Justiz haben. Aus diesem Grund hat sich die Justizverwaltungsleitung des Kantons Bern als gemeinsames Organ von Obergericht, Verwaltungsgericht und Generalstaatsanwaltschaft eng an der Ausarbeitung der vorliegenden Vernehmlassung des Kantons beteiligt. Mehrere der nachfolgenden Anträge und Formulierungsvorschläge beruhen auf Vorschlägen der Justizverwaltungsleitung.

In grundsätzlicher Hinsicht regen wir ausserdem Folgendes an: Die VEKJ enthält zahlreiche Vorschriften mit stark technischem Charakter. Wir regen an, zu überdenken, ob einzelne Regelungen, die aufgrund des raschen technischen Wandels zeitnah an die neuen Entwicklungen angepasst werden müssen, nicht mit Vorteil in einer Verordnung des EJPD statt in der VEKJ zu regeln wären.

2. Anträge

1.1 Antrag zum Ingress

Im Ingress seien alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen.

1.2 Begründung

Im Vorentwurf fehlen bewusst die Artikel, die dem Bundesrat die Kompetenz zur Regelung des Formats der elektronisch übermittelten Dokumente übertragen. Im Erläuternden Bericht wird präzisiert, dass, «um die Übersichtlichkeit zu bewahren», im Ingress lediglich die Bestimmungen der Verfahrensgesetze erwähnt würden, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben. Auch wenn ein allgemeiner Verweis auf das BEKJ sinnvoll erscheint, wäre es vorzuziehen, alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen. Dies gilt insbesondere für die Artikel, die dem Bundesrat die Kompetenz zur Festlegung der Formate übertragen; diese sollten daher ebenfalls im Ingress erwähnt werden.

Der Ingress sollte daher wie folgt ergänzt werden (Ergänzungen unterstrichen):

Der Schweizerische Bundesrat,

gestützt auf das Bundesgesetz vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ),

die Artikel 6a Absatz 2, 21a Absatz 2 und 34 Absatz 1bis des Verwaltungsverfahrensgesetzes vom 20.Dezember 1968 (VwVG),

Artikel 38e des Bundesgerichtsgesetzes vom 17. Juni 2005 (BGG),

die Artikel 128b Absatz 3, 128c Absatz 2 und 128e der Zivilprozessordnung (ZPO),

die Artikel 33a Absatz 4, 33b, 33c Absatz 2 und 34 Absatz 3 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG),

die Artikel 76a Absatz 2, 103b Absatz 3, 103c Absatz 2 und 103e der Strafprozessordnung (StPO),

Artikel 2e des Bundesgesetzes vom 23. Dezember 2011 über den ausserprozessualen Zeugenschutz (ZeugSG),

Artikel 31f des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR),

die Artikel 8c Absatz 3, 8d Absatz 2 und 8f des Opferhilfegesetzes vom 23. März 2007 (OHG)

und die Artikel 37d und 38a Absatz 2 des Militärstrafprozesses vom 23. März 1979 (MStP),

verordnet: ....

2.1 Antrag zu Art. 2 Abs. 1 Bst. b

Art. 2 Abs. 1 Bst. b sei wie folgt zu formulieren: «Die Übermittlung sämtlicher Daten (Up- und Download) sowie deren Speicherung auf der Plattform erfolgen verschlüsselt gemäss *[Verweis auf die generell abstrakte Regelung der anzuwendenden Standards].*»

2.2 Begründung

Aus unserer Sicht ist zu wenig klar, welche technischen Standards gemeint sind. Die Erwähnung einer entsprechend generell abstrakt formulierten (rechtlichen) Grundlage der anzuwendenden Standards (Verordnung, Weisung, oder Ähnliches) wäre aus unserer Sicht anzustreben, zumal es eine solche geben dürfte, um deren Verbindlichkeit innerhalb der Bundesverwaltung zu gewährleisten. Ein Verweis im Erläuternden Bericht auf die Website «Vorgaben der Bundeskanzlei» ist unseres Erachtens nicht ausreichend. Zudem werden nach unserem Verständnis zwei Sachen vermischt, die technologisch zu unterscheiden sind: Übermittlung und Speicherung.

3.1 Antrag zu Art. 2 Abs. 1 Bst. c

Buchstabe c sei zu streichen.

3.2 Begründung

Die Justizverwaltungsleitung befürchtet, dass die Begrenzung auf zwei Gigabyte die Einreichung von grösseren Dateien (z.B. grössere Videodateien) als Beweismittel verunmöglicht. Falls die Begrenzung aus technischen Gründen unumgänglich ist, schlagen wir vor, die Begrenzung deutlich zu erhöhen.

4.1 Antrag zu Art. 2 Abs. 1 Bst. d

Art. 2 Abs. 1 Bst. d sei umzuformulieren, damit er die Regelungsabsicht besser zum Ausdruck bringt.

4.2 Begründung

Wie der erläuternde Bericht auf Seite 11 zurecht ausführt, wird durch die Löschfunktion nur die erteilte individuelle *Berechtigung* gelöscht, nicht jedoch das Dokument als solches. Der Wortlaut der Bestimmung ist deshalb zu absolut formuliert und sollte umformuliert werden, damit besser zum Ausdruck kommt, dass nur die Berechtigung entzogen wird.

5.1 Anträge für eine Ergänzung von Art. 2 Abs. 1

5.1.1 Antrag 1

Art. 2 Abs. 1 sei mit einer zusätzlichen Vorschrift (neuer Buchstabe) zur Protokollierung der Aktivitäten zu ergänzen. Diese sollte folgenden Inhalt aufweisen:
Die Plattform protokolliert sämtliche Aktivitäten, damit jederzeit nachvollzogen werden kann,

- *welcher Benutzer bzw. welche Benutzerin zu welchem Zeitpunkt welche Aktivitäten vorgenommen hat (Login, Logout, Up- und Download von Daten, Löschen von Daten, Mutationen, Änderung von Metadaten); dies zwecks Sicherstellung der Nachvollziehbarkeit,*
- *wann und bei welcher Aktivität technische Fehler aufgetreten sind (z.B. beim Versuch, eine zu grosse Datei hochzuladen, oder eine, die kein gültiges Dateiformat aufweist etc.).*

5.1.2 Begründung

In Absatz 1 von Art. 2 sollte in einer zusätzlichen Bestimmung die Protokollierung aller Aktivitäten festgehalten werden, damit jederzeit nachvollzogen werden kann, wer was gemacht hat. Im Erläuternden Bericht zu Art. 2 Abs. 1 Bst. a steht ausdrücklich, dass die Plattformen die bei ihnen gespeicherten Dokumente so sichern müssen, dass Unbefugte weder darauf zugreifen noch sie verändern können. Dies umfasse technische Massnahmen wie Verschlüsselung, Zugriffssteuerung und Protokollierung von Zugriffen und Zugriffsversuchen.

5.2.1 Antrag 2

Art. 2 Abs. 1 sei mit einer zusätzlichen Vorschrift (neuer Buchstabe) zu den Vorgaben zur Interoperabilität der Plattformen zu ergänzen.

5.2.2 Begründung

Art. 25 Abs. 2 BEKJ verlangt die Interoperabilität unter allen Plattformen. Gemäss Art. 25 Abs. 3 BEKJ regelt der Bundesrat die Anforderungen an die Interoperabilität sowie das Bewilligungsverfahren und die Kostentragung. Während der E-VEKJ in Art. 3 Bestimmungen zum Bewilligungsverfahren und der Kostentragung enthält, fehlen nach unserer Auffassung entsprechende detaillierte Bestimmungen zur geforderten Interoperabilität. Gemäss Art. 3 Abs. 2 E-VEKJ wird eine Betriebsbewilligung erteilt, wenn die Anforderungen nach Art. 2 erfüllt sind (vgl. auch Art. 25 Abs. 2 BEKJ). Entsprechend sind die gemäss Art. 25 BEKJ zu regelnden Vorgaben zur Interoperabilität in Art. 2 VEKJ zu ergänzen, weil deren Erfüllung für den Erhalt der Betriebsbewilligung vorausgesetzt wird.

6.1 Antrag zu Art. 4

In der VEKJ sei an geeigneter Stelle in einer allgemeinen Bestimmung darauf hinzuweisen, dass mit «Dokument» technisch «Datei» gemeint ist.

6.2 Begründung

Der Vorentwurf verwendet – wie das BEKJ – den Begriff «Dokument» anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: «Der Begriff "Datei" ist für das Gesetz zu technisch.» Damit sind wir grundsätzlich einverstanden. Indessen sollte in einer allgemeinen Bestimmung gesagt werden, in welchen Artikeln der VEKJ mit dem Begriff «Dokument» technisch «Datei» gemeint ist. Im Erläuternden Bericht sollten dazu Ausführungen gemacht werden.

7.1 Antrag zu Art. 4 Abs. 2 bis 5

Die Formate für Beilagen sind in Einklang mit Abs. 3 zu standardisieren.

7.2 Begründung

Den Parteien wird in Art. 4 Abs. 2 freigestellt, *Beilagen in einem beliebigen Format* einzureichen. Die verfahrensleitende Behörde muss *mindestens* die in Abs. 3 festgehaltenen Formate bearbeiten können. Können die Beilagen von der verfahrensleitenden Behörde nicht zweckmässig bearbeitet werden, kann die Verfahrensleitung festlegen, in welchem Format Beilagen eingereicht werden müssen (Abs. 4). Aus dem Wortlaut (insbesondere von Abs. 2) ist zu schliessen, dass auch *andere Formate als die in Abs. 3 genannten* eingereicht werden können. Wenn die Behörde diese Beilagen trotzdem bearbeiten kann, muss sie nichts unternehmen und muss nicht nach Abs. 4 vorgehen. Sie ist jedoch nicht verpflichtet, diese anderen Formate bearbeiten zu können. Ihre Pflicht beschränkt sich auf die Formate gemäss Abs. 3.

Vorausgesetzt, wir haben den Zusammenhang zwischen den Absätzen 2, 3 und 4 richtig verstanden, sind wir der Ansicht, dass die getroffene Regelung nicht sachgerecht ist. Es kann Leerläufe verursachen, wenn Parteien aufgefordert werden müssen, eingereichte Beilagen in einem anderen Format neu einzureichen. Im Übrigen besteht auch die Möglichkeit, dass nicht nur verfahrensleitende Behörden, sondern auch *Verfahrensbeteiligte* gewisse Formate nicht öffnen können. Es könnte mit einer *Begrenzung der zulässigen Formate für Beilagen* Rechtsklarheit für alle Verfahrensbeteiligte geschaffen und Verfahrensverzögerungen entgegengewirkt werden. Vor diesem Hintergrund bitten wir darum, nicht sämtliche Formate für Beilagen zuzulassen, sondern sie zu standardisieren. Dabei ist denkbar, dass die Verfahrensbeteiligten in begründeten *Ausnahmefällen* Beilagen in weiteren Formaten einreichen dürfen, falls ein Beweismittel nicht in eines der zugelassenen Formate umgewandelt werden kann, ohne dass der Beweiswert eingeschränkt wird. Voraussetzung ist, dass die Behörde dieses Format bearbeiten kann. Der Grundsatz von Abs. 2 ist somit umzukehren: Zulässig ist ein numerus clausus von Formaten, von dem es aber Ausnahmen gibt. Damit wäre dennoch dem Grundsatz Rechnung getragen, dass die Form der Beweismittel grundsätzlich nicht beschränkt wird.

8.1 Anträge zu Art. 5

8.1.1 Antrag 1

In Abs. 1 sei «einzelne» Quittung durch «einzige» Quittung zu ersetzen.

8.1.2 Antrag 2

In Abs. 2 Bst. d sei Ziff. 2 zu streichen.

8.2 Begründung

Abs. 1: Aus Sinn und Zweck der Bestimmung und aus dem Erläuternden Bericht geht hervor, dass die Plattform bei mehreren übermittelten Dokumenten *eine einzige* Quittung ausstellt.

Abs. 2 Bst. d: Ziff. 2 dieser Bestimmung hält fest, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung auszuweisen bzw. aufzulisten sind. Die Bestimmung enthält unseres Erachtens einen logischen Fehler: Nicht übermittelte Dokumente können auf der Eingangsquittung nicht aufgeführt werden, da diese eben nicht übermittelt wurden. Die Quittung kann keine Hashwerte von Dateien enthalten, welche nicht übermittelt worden sind. Kann die

Plattform ein Dokument oder mehrere Dokumente nicht übermitteln, so erhält die Absenderin oder der Absender bloss eine *Mitteilung* der Plattform, jedoch keine Quittung. Die Ziff. 2 ist daher zu streichen.

9.1 Anträge zu Art. 6 und Art. 7

Der Widerspruch zwischen dem Verordnungstext von Art. 6 und dem Erläuternden Bericht sei zu bereinigen. Weiter ist im Verordnungstext und in den Materialen zu präzisieren, welche elektronischen Dokumente (bzw. Dateien) zwingend mit einem Siegel zu versehen sind und durch welche Stellen dies zu erfolgen hat.

9.2 Begründung

Nach dem Wortlaut von Art. 6 reicht es, dass nur *ein* Dokument über ein Siegel und einen Zeitstempel verfügt, wenn eine Behörde *mehrere* Dokumente zusammen an eine Plattform übermittelt. Im Erläuternden Bericht dazu wird festgehalten, dass beim Versand durch eine Behörde diese *alle* Dokumente mit einem Siegel und einem Zeitstempel versehen muss. Dokumente, die bereits über eine qualifizierte elektronische Signatur oder ein geregeltes elektronisches Siegel zusammen mit einem qualifizierten elektronischen Zeitstempel verfügen, braucht die Behörde *nicht erneut zu siegeln*. Diese Aussage entspricht nicht dem Inhalt von Art. 6, in dem steht, dass nur *eines von mehreren* Dokumenten gesiegelt sein muss. Der Erläuternde Bericht sagt aber, dass doch *alle* Dokumente zu siegeln sind mit *Ausnahme* derjenigen, die bereits ein Siegel haben. Wir bitten Sie, diesen Widerspruch zu aufzulösen.

Art. 6 spricht nur von «Dokumenten», die von einer «Behörde» übermittelt werden. Der Text lässt aber offen, ob sämtliche Dokumente gemeint sind – worauf der Erläuternde Bericht hindeutet – oder nur eine bestimmte Art. Zwingend zu siegeln sind insbesondere Entscheide, Verfügungen und andere behördliche Akte, die unmittelbar Rechte und Pflichten begründen, ändern, aufheben oder verbindlich feststellen. Art. 6 sollte dazu eine ausdrückliche Regelung vorsehen. Weiter ist unklar, ob sämtliche Behörden die fraglichen Dokumente siegeln müssen oder ob die Vorschrift nur bestimmte Behörden betrifft. Zu unterscheiden ist – wie der Erläuternde Bericht zurecht erwähnt – insbesondere zwischen verfahrensleitenden und verfahrensbeteiligten Behörden. Art. 6 sollte ausdrücklich erwähnen, welche Behörden ein Siegel anbringen müssen.

Der Erläuternde Bericht zu Art. 7 führt aus, dass ein direkt in übermittelten Dokumenten angebrachtes Siegel die Dokumente verändere. Werde das Siegel in einem separaten Dokument angebracht, würden die übermittelten Dokumente unverändert bleiben. Unklar ist jedoch, weshalb dies nur bei *mehreren* Dokumenten ein Problem sein soll bzw. nur bei mehreren übermittelten Dokumenten das Siegel in einem separaten Dokument angebracht werden soll, nicht aber bei einer Eingabe, die aus einem einzigen Dokument besteht. Wir bitten Sie, dies zu erläutern. Aus Art. 7 und dem Erläuternden Bericht sollte klar hervorgehen, welche Dokumente der Eingabe (die Eingabe selbst und/oder die Beilagen) von der Plattform gesiegelt werden und in welchen Fällen (und weshalb) die Siegelung nicht auf dem Dokument erfolgt, sondern auf einem separaten Dokument.

Im Zusammenhang mit der Übermittlung von behördlichen Dokumenten an Personen, die nicht elektronisch mit dem Gericht oder der Behörde kommunizieren, führen Sie in Ziff. 2.6 des Erläuternden Berichts Folgendes aus: Die Regulierungsidee, anstelle eines eigenhändig unterschriebenen Entscheids auf Verordnungsstufe auch den Versand eines Ausdrucks des elektronischen

Originals zuzulassen, sei verworfen worden. Sie schreiben, dass beispielsweise die mit dem BEKJ indirekt geänderten Art. 238 Bst. h ZPO und Art. 353 Abs. 1 Bst. k StPO explizit vorschreiben würden, dass eine Unterschrift bei Papierversand notwendig sei. Für eine abweichende Regelung auf Verordnungsstufe verbleibe kein Spielraum. Auch wenn wir diese Ausführungen nachvollziehen können, bitten wir Sie auf Wunsch der Justizverwaltungsleitung gleichwohl nochmals zu prüfen, ob für den Versand eines Papierausdrucks des elektronischen Originals ohne Handunterschrift tatsächlich kein Spielraum besteht. Die Justizverwaltungsleitung würde eine solche Lösung aus praktischen Gründen klar bevorzugen; in die gleiche Richtung äussert sich auch die Arbeitshilfe von Justitia 4.0 für die Kantone.

10.1 Antrag zu Art. 8 Abs. 3

Der Begriff «angemessenes» sei durch «gleichwertiges» zu ersetzen.

10.2 Begründung

Der Begriff «angemessenes Schutzniveau» ist zu wenig bestimmt. Die anderen Authentifizierungsdienste sollten ein Schutzniveau haben, das gleichwertig wie dasjenige von Abs. 1 ist. Das würde der Anforderung von Abs. 2 entsprechen, der für die Plattformen der Kantone nach Art. 1 Bst. b eine «*mindestens so hohe* Authentifizierungsqualität» verlangt.

11.1 Anträge zu Art. 9

11.1.1 Antrag 1

In Art. 9 sei der Unterschied zwischen den *Adressen* von Behörden und Personen (Art. 18 BEKJ), *Benutzern und Benutzergruppen* (Art. 24 BEKJ) und *Profilen* (Art. 9 VEKJ) klarzustellen.

11.1.2 Antrag 2

Die Postadresse sei bei allen Profilen zu streichen.

11.2 Begründung

Die organisatorischen und technischen Abhängigkeiten resp. Zusammenhänge folgender Bestimmungen sind unklar:
Art. 18 BEKJ sieht vor, dass die Plattform ein Verzeichnis mit den *Adressen* aller Behörden und Personen enthält, welche über die Plattform kommunizieren. Es ist hier explizit nicht von Benutzern bzw. Benutzerinnen die Rede. Art. 24 BEKJ gibt vor, dass die Plattform eine Stellvertretungsfunktionalität zwischen einzelnen Benutzern zur Verfügung stellen muss. Zudem sollen *Benutzer* Benutzergruppen erstellen können. Art. 9 VEKJ soll nun weiter ermöglichen, dass die Benutzerinnen und Benutzer auf der Plattform in ihrem Konto mehrere Profile anlegen können, wobei zwischen Profilen von Behörden und übrigen Benutzern (natürliche Personen und Organisationen) unterschieden wird. Der Begriff des «Profils» kommt im BEKJ nicht vor.
Weder aus dem Verordnungstext noch aus dem Erläuternden Bericht wird klar, wie

- die Adressen von Behörden und Personen (Art. 18 BEKJ),

- die Benutzer bzw. Benutzerinnen und Benutzergruppen (Art. 24 BEKJ), und
- die Profile (Art. 9 VEKJ) zueinander stehen.

Hier ist unseres Erachtens Klärungsbedarf gegeben.
Nach unserem Verständnis sollte die Struktur grundsätzlich nach folgendem Prinzip aufgebaut sein:
1. und oberste Ebene: *Adressen* von Behörden und Personen. Z.B. Regionalgericht Bern-Mittelland oder Anwaltskanzlei Recht & Partner.
2. Ebene: (Funktionsspezifische) *Profile*, die durch die obere Ebene vorgegeben werden, z.B. Strafabteilung, Team SchKG, Team RA Muster, etc.
3. Ebene: *Benutzer*: Mitarbeiterin X, Kanzleichefin Y, Gerichtspräsidentin Z, etc.

Die Postadresse sollte aus unserer Sicht bei allen Profilen gestrichen werden, da sie im elektronischen Kontext irrelevant ist. Die Zustelladresse auf der Plattform ist eindeutig und ausreichend. Auf Behördenseite ist die Erfassung der Postadresse v.a. in denjenigen Fällen schwierig, in denen es verschiedene Standorte, aber nur eine Zustelladresse auf der Plattform gibt.

12.1 Antrag zu Art. 11

Die Justizverwaltungsleitung regt an, Art. 11 sei mit einem neuen Absatz 3 wie folgt zu ergänzen:
«Die im Adressverzeichnis aufgeführten Behörden und Personen, die über die Plattform kommunizieren, sind dafür verantwortlich, dass die ihnen zugeordneten Profile auf der Plattform jederzeit über die aktuellen Mitglieder verfügen und keine Mitglieder enthalten, die nicht mehr bei ihnen tätig sind.»

12.2 Begründung

Die Aufforderung der Plattform an die Benutzerinnen und Benutzer, ihre eigenen Berechtigungen zu überprüfen, reicht unseres Erachtens nicht aus. Viel wichtiger ist es, die Behörden und Personen, welche im Adressverzeichnis gemäss Art. 18 BEKJ eingetragen sind, aufzufordern, die zu ihrer Organisation gehörenden Benutzerinnen und Benutzer zu überprüfen. Die Kanzleimitarbeiterin, welche ihre Anstellung in der Anwaltskanzlei gekündigt hat, wird sich unter Umständen nicht selbst melden resp. die Aufforderung der Plattform gar nicht mehr sehen. Gleich verhält es sich mit dem Gerichtsmitarbeiter, welcher pensioniert wird. Die Verantwortung und Möglichkeit zur Mutation von Benutzerinnen und Benutzer dürfen nicht (nur) bei diesen selber liegen.

13.1 Antrag zu Art. 12

Artikel 12 sie wie folgt zu ändern bzw. zu ergänzen:
Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen
[1] Die auf einer Plattform gespeicherten Dokumente ~~und Quittungen~~ werden sechs Monate nach der Entgegennahme ~~beziehungsweise nach der Erstellung~~ automatisch vernichtet.
[2] Stehen Dokumente zur Akteneinsicht zur Verfügung, so bestimmt die verfahrensleitende Behörde, wie lange die Dokumente auf der Plattform abrufbar sind. Nach Ablauf der Frist werden die Dokumente automatisch ~~vernichtet~~ gelöscht.
[3] Quittungen werden drei Jahre nach ihrer Erstellung automatisch gelöscht.

13.2 Begründung

Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein «Briefkasten» und keine Langzeitablage sein soll. Bei den Quittungen ist es dagegen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Grundsätzlich müssen die Behörden darum besorgt sein, die Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch aufgrund der Funktionsweise der zentralen Plattform – etwa im Fall von Zustellungen – dazu kommen, dass das Herunterladen der Quittungen unterbleibt. Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von der Plattform selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen.

Quittungen können Personendaten enthalten (so etwa die Namen von Verfahrensbeteiligten), was diese im Kontext von Justizverfahren unter Umständen zu besonders schützenswerten Personendaten macht. Jedoch sind diese Daten, wie auch die weitaus sensibleren Aktenstücke selbst, auf der Plattform verschlüsselt gespeichert. Hinzu kommt, dass es sich bei Quittungen um sehr kleine Datenmengen handelt, die keinen hohen zusätzlichen Speicherbedarf verursachen, selbst wenn sie lange auf der Plattform verfügbar bleiben müssen.

In Anlehnung an die Zeitspanne von drei Jahren, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind, wird vorgeschlagen, Artikel 12 gemäss dem obenstehenden Antrag zu ändern.

14.1 Antrag zu Art. 13

Art. 13 ist mit der Angabe des Kapitels des Informationssicherheitsgesetzes, zu dem der 3. Abschnitt gehört, zu ergänzen.

14.2 Begründung

Die fragliche Bestimmung verweist auf den 3. Abschnitt des Informationssicherheitsgesetzes, die Angabe des relevanten übergeordneten Kapitels (2.?), zu dem der 3. Abschnitt gehört, fehlt aber und sollte ergänzt werden.

15. Anträge zu Art. 14

15.1.1 Antrag 1

Der Begriff der Viren ist durch den Überbegriff «Schadsoftware» zu ersetzen.

15.1.2 Begründung

Der Begriff «Viren» ist zu eng gefasst und sollte durch den weiter gefassten Oberbegriff «Schadsoftware» (englisch: Malware) ersetzt werden. Nebst Viren gibt es noch andere Arten

von Schadsoftware (z.B. Ransomware, Trojaner, etc.), vor denen die Dokumente auf der Plattform ebenfalls geschützt werden sollten.

15.2.1 Antrag 2

Absatz 1 ist wie folgt abzuändern:
[1] Die Plattformen ~~müssen bei bis zu 64 Megabyte grossen Dateien~~ führen eine Virenprüfung ~~durchführen~~.

15.2.2 Begründung

Die Festlegung der (Maximal-)Grösse von prüfbaren Blöcken grösserer Dateien sollte nicht öffentlich kommuniziert werden. Diese Information ist für die Nutzerinnen und Nutzer der Plattform irrelevant. Sie eröffnet potenziellen Angreifern die Möglichkeit, ihre Schadsoftware in einer verseuchten Datei so anzuordnen, dass der Schadcode bei der Aufspaltung in mehrere Blöcke in zwei aufeinanderfolgenden Blöcken liegt und nicht zuverlässig als schädlich erkannt werden kann. Zudem wird es stark von der für die Aufspaltung und Prüfung zuständigen Software abhängen, wie gross diese prüfbaren Blöcke zu gestalten sind. Diese Grenze wird sich aufgrund von Betriebserfahrung und Verbesserungen in der Hard- und Software verändern und sollte einfach anpassbar sein.

15.3.1 Antrag 3

Absatz 2 ist zu streichen.

15.3.2 Begründung

Der Grenzwert für eine vollständige Prüfung auf Schadsoftware von derzeit 64 MB kann (und sollte) basierend auf den technischen Möglichkeiten und der wachsenden Betriebserfahrung durch die Betreiber der Plattformen erhöht werden können. Absatz 2 ist daher zu streichen.

15.4.1 Antrag 4

In Absatz 3 sollte klargestellt werden, in welchen Fällen auf eine Virenprüfung verzichtet werden kann und wie die Plattformbetreiberin diesen Entscheid trifft.

15.4.2 Begründung

Nach Auffassung der Justizverwaltungsleitung geht es bei der Bestimmung von Abs. 3 um Situationen, in welchen die Gründe für einen ausnahmsweisen Verzicht auf eine Virenprüfung im Verfahren selbst liegen (z.B. Schadsoftware als Teil der Beweismittel). Damit stellt sich die Frage, wie die Betreiberin der Plattform diesen Verfahrensbezug zuverlässig überprüfen kann. Es wäre somit sinnvoll, wenn dieses Thema noch detaillierter geregelt und im Erläuternden Bericht erläutert würde. Auf Anregung der Justizverwaltungsleitung schlagen wir vor, den Absatz 3 mit konkreten Voraussetzungen zu ergänzen, bei deren Erfüllung auf eine Virenprüfung verzichtet werden kann.

15.5.1 Antrag 5

Absatz 4 sollte wie folgt lauten:
[4] Dokumente, bei denen ~~eine Virenprüfung nach Absatz 2~~ keine oder eine eingeschränkte Virenprüfung durchgeführt wurde, müssen entsprechend gekennzeichnet werden.

15.5.2 Begründung

Eine klare Kennzeichnung ist auch dann wichtig, wenn die Virenprüfung nur eingeschränkt stattgefunden hat. Absatz 4 ist dementsprechend zu ergänzen. Offen bleibt allerdings, wie die Ergebnisse der Virenprüfung den Nutzenden mitgeteilt werden. Die Mitteilung sollte technisch einfach und inhaltlich leicht verständlich erfolgen können.

16.1 Antrag zu Art. 15

Art. 15 sei wie folgt neu zu fassen:
[1] ~~Die Gesamthöhe~~ Der Gesamtbetrag der jährlich von den Mitgliedern der öffentlich-rechtlichen Körperschaft zu entrichtenden Gebühr ~~für die Nutzung der zentralen Plattform~~ muss die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform decken und die Bildung einer Reserve für die Sicherstellung der Liquidität der öffentlich-rechtlichen Körperschaft in der Höhe von 10 Prozent der jährlichen Betriebskosten ~~ermöglichen~~ gewährleisten.
[Anpassung und neuer Absatz 2]
[2] ~~Die Einnahmen aus Leistungsbezügen der~~ Beiträge von Kantonen, die nicht Mitglied der öffentlich-rechtlichen Körperschaft sind, werden vom Gesamtbetrag der jährlichen Gebühr abgezogen.
[3] Das EJPD legt ~~die jährliche~~ den Gesamtbetrag der jährlichen Gebühr ~~aufgrund~~ für jeweils drei Jahre im Voraus auf der Grundlage der Finanzplanung der öffentlich-rechtlichen Körperschaft fest.
[4] Das EJPD kann die Gebühr während der Periode nach Absatz 3 ~~2~~ anpassen, wenn die eingenommenen Beiträge nach Absatz 1 und 2 ~~diese Gebühr~~ die Betriebs- und Weiterentwicklungskosten nicht ~~deckt~~ decken oder die Reserve die Limite nach Absatz 1 überschreitet.

16.2 Begründung

Die deutsche und die französische Fassung sollten in Übereinstimmung gebracht werden. Für denselben Sachverhalt sollte eine einheitliche Terminologie gewählt werden. Der Absatz 1 sollte der Klarheit halber in (neu) zwei Absätze aufgeteilt werden.

17.1 Antrag zu Art. 16

Art. 16 sei wie folgt neu zu fassen
[1] Die Gesamthöhe der Gebühr wird wie folgt auf den Bund und die Kantone, die Mitglied der öffentlich-rechtlichen Körperschaft sind, aufgeteilt:
a. Bundesverwaltung und Bundesanwaltschaft: 5 Prozent;
b. Eidgenössische Gerichte: 5 Prozent;
c. Kantone: 90 Prozent.

[2] Der Anteil der Kantone wird ~~gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt~~ unter den Kantonen, die Mitglieder der öffentlich-rechtlichen Körperschaft sind, proportional zu deren ständigen Wohnbevölkerung am 1. Januar des Vorvorjahres, für das die Gebühr fällig wird, verteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen ~~im Zeitpunkt der Festlegung nach Artikel 15~~.
[3] Das EJPD legt jährlich die Verteilung der Gebühr auf die Kantone fest.

17.2 Begründung

Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 Prozent wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Falls diese Zahl höher sein wird als erwartet, müsste der Bundesanteil erhöht werden. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die *Aufteilung* der Gebühr gemäss Art. 16 sollte Gegenstand der Prüfung sein, und nicht nur die Berechnung gemäss Art. 15.

Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen. Anhand dieser verbindlichen Angaben legt das EJPD den jährlichen Gebührenbeitrag fest; es berücksichtig dabei die in Artikel 15 Absatz 4 definierten Schwellenwerte und den allfälligen Beitritt eines Nichtmitgliedes zur Körperschaft justitia.swiss nach deren Gründung (vgl. Art. 19 Vereinbarung justitia.swiss).

18.1 Antrag zu Art. 19

Art. 19 sei wie folgt neu zu fassen:
[1] Die jährliche Gebühr der Mitglieder der öffentlich-rechtlichen Körperschaft ist ~~sind~~ im Voraus zu entrichten und am 1. Januar fällig.
[2] Die Gebühr für ~~das erste Betriebsjahr der öffentlich-rechtlichen Körperschaft ist an dem Tag fällig, an dem diese Verordnung in Kraft tritt~~ die Nutzung der zentralen Plattform ist erstmals am Tag des Inkrafttretens dieser Verordnung fällig.
[3] Die Bestimmungen des Obligationenrechts zum Schuldnerverzug finden sinngemäss Anwendung.

18.2 Begründung

In Absatz 2 sollte nicht das Betriebsjahr der öffentlich-rechtlichen Körperschaft genannt werden, sondern die *Nutzung der zentralen Plattform*. Die Gebühr wird für Nutzung der Plattform erhoben und nicht für den Betrieb der Körperschaft.
Die Verordnung lässt die weiteren Modalitäten der Erfüllung offen. Es ist anzunehmen, dass die Regeln des Obligationenrechts sinngemäss zur Anwendung kommen.

19.1 Antrag zu Art. 22

Die Justizverwaltungsleitung regt an, Art. 22 sei ab Absatz 3 wie folgt abzuändern und zu ergänzen:
[3] Die Dokumente sind, soweit dies technisch möglich und für die jeweilige Vorlage geeignet ist, mittels Texterkennung durchsuchbar zu machen. Die Texterkennung dient der Auffindbarkeit und Weiterverarbeitung; sie ist nicht Teil der für die Übereinstimmung nach Absatz 4 massgebenden Bildebene.
[4] Das sichtbare digitale Abbild muss vollständig, lesbar und dem physischen Dokument bildlich entsprechend sein. Die Qualitätssicherung umfasst insbesondere Vollständigkeit, Lesbarkeit, Seitenfolge, Farbwiedergabe, Auflösung, Behandlung von Sonderfällen und Dokumentation von Nachscans. Sie umfasst keine inhaltliche Prüfung der mittels digitaler Nachbearbeitung erzeugten weiteren Layer.
[5] Wurde ein Digitalisat in einem dokumentierten Verfahren erstellt, mit einem qualifizierten elektronischen Zeitstempel versehen und nach Absatz 4 qualitätsgesichert, wird vermutet, dass es dem physischen Dokument bildlich entspricht. Die Vermutung entfällt bei konkreten gegenteiligen Anhaltspunkten.
[6] Das EJPD bezeichnet oder konkretisiert die Mindestanforderungen an Prozessdokumentation, Stichproben, Fehlerbehandlung, Nachscan, Protokollierung und Verantwortlichkeiten. Es berücksichtigt hierfür anerkannte Standards, namentlich die BSI TR03138 RESISCAN oder gleichwertige Standards.

19.2 Begründung

Die Formulierung von Art. 22 ist nach Auffassung der Justizverwaltungsleitung in den Kernpunkten zu unbestimmt und sollte daher ergänzt werden. Die Justizverwaltungsleitung begründet das Anliegen wie folgt: Die Formulierung verbinde Mindestwerte für OCR, Farbtiefe und Auflösung mit der Forderung nach bildlicher und inhaltlicher Übereinstimmung, ohne den Massstab der Qualitätskontrolle festzulegen. Daraus resultiere eine faktisch nur schwer erfüllbare Pflicht zur Kontrolle des OCR-Layers. OCR erhöhe zwar die Nutzbarkeit, könne aber bei Handschriften, Stempeln, Formularen, Tabellen, schlechten Vorlagen oder Mischdokumenten nicht denselben Verlässlichkeitsgrad wie das sichtbare Abbild gewährleisten. Die Anlehnung an den deutschen Standard RESISCAN erscheine sinnvoll, weil damit nicht nur technische Mindestwerte, sondern ein vollständiger Prozessansatz abgebildet werde: Vorbereitung, Scan, Vollständigkeitskontrolle, Umgang mit Sonderfällen, Protokollierung, Nachscan, Freigabe und Verantwortlichkeit. Im Übrigen sollten technische Details in einer Departementsverordnung geregelt werden.

Für die Begründung im Erläuternden Bericht schlägt die Justizverwaltungsleitung folgende Formulierung vor:
«Die Qualitätskontrolle bezieht sich auf das sichtbare digitale Abbild des physischen Dokuments. Sie umfasst insbesondere Vollständigkeit, Lesbarkeit, Seitenfolge, korrekte Zuordnung, Umgang mit Sonderformaten und Dokumentation von Nachscans. Der mittels Texterkennung erzeugte Textlayer dient der Auffindbarkeit und Weiterverarbeitung. Er ist nicht massgebend für die beweisrechtliche Übereinstimmung mit dem physischen Dokument und muss nicht inhaltlich vollständig kontrolliert werden.

Für die Ausgestaltung des Digitalisierungsverfahrens können anerkannte Standards beigezogen werden, namentlich die BSI TR-03138 RESISCAN oder gleichwertige Standards. Entscheidend ist ein dokumentierter, risikobasierter End-to-End-Prozess. Wird ein Digitalisat nach einem sol-

chen Verfahren erstellt und qualitätsgesichert, spricht eine Vermutung für die bildliche Richtigkeit und Vollständigkeit des Scans, solange keine konkreten gegenteiligen Anhaltspunkte bestehen.»

20.1 Antrag für einen neuen Art. 22a

Die Justizverwaltungsleitung regt an, die Verordnung sei mit einem neuen Art. 22a wie folgt zu ergänzen:
Art. 22a Bereits bestehende digitale Aktenstücke und Dossiers
[1] Digitale Aktenstücke und digitale Dossiers, die vor Inkrafttreten dieser Verordnung oder ausserhalb des Verfahrens nach Artikel 22 erstellt wurden, können als elektronische Aktenstücke beziehungsweise elektronische Dossiers im Sinne des BEKJ verwendet werden, wenn sie eindeutig zugeordnet, vollständig, lesbar und unverändert in die elektronische Akte übernommen werden können.
[2] Die zuständige Behörde dokumentiert die Übernahme summarisch. Die Dokumentation enthält mindestens die Herkunft des Dossiers, den Zeitpunkt der Übernahme, das übernehmende System und allfällige festgestellte Einschränkungen.
[3] Eine erneute Digitalisierung der Papierunterlagen ist nicht erforderlich, wenn die Voraussetzungen nach Absatz 1 erfüllt sind oder wenn keine Papierunterlagen mehr verfügbar sind und keine konkreten Zweifel an Vollständigkeit oder Lesbarkeit bestehen.
[4] Bestehen konkrete Zweifel an Vollständigkeit, Lesbarkeit oder Zuordnung, ordnet die Behörde eine angemessene Nachprüfung, Ergänzung oder erneute Digitalisierung an.

20.2 Begründung

Die Justizverwaltungsleitung hält dazu fest, dass bereits heute trotz Papierprimat in vielen Verfahren vollständige elektronische Arbeitsdossiers erstellt werden. Würden diese nach Inkrafttreten des BEKJ nicht als vollwertige digitale Dossiers verwendbar sein, entstünden unnötige Doppelerfassungen, Medienbrüche und Ressourcenverluste. Aus diesem Grund sei eine pragmatische Regelung vorzusehen, wonach keine rückwirkende Zertifizierung aller Altbestände, aber eine nachvollziehbare Übernahme mit summarischer Dokumentation und Nachprüfung nur bei konkreten Zweifeln eingeführt werden solle.

Zur Begründung im Erläuternden Bericht schlägt die Justizverwaltungsleitung folgende Formulierung vor:
«Bereits vor Inkrafttreten der Verordnung erstellte elektronische Arbeitsdossiers, Legacy-Scans und anderweitig entstandene digitale Aktenbestände sollen ohne erneute Digitalisierung weiterverwendet werden können. Die Übernahme setzt keine rückwirkende Zertifizierung voraus. Erforderlich ist eine angemessene Dokumentation der Herkunft, Übernahme, Vollständigkeit und Lesbarkeit. Nur bei konkreten Zweifeln ist eine Nachprüfung, Ergänzung oder erneute Digitalisierung vorzunehmen.»

21.1 Antrag für einen neuen Art. 22b

Die Justizverwaltungsleitung regt an, die Verordnung sei mit einem neuen Art. 22b wie folgt zu ergänzen:
Art. 22b Rücksendung physisch eingereichter Dokumente

[1] Von der Rücksendung physisch eingereichter Dokumente nach Artikel 30 Absatz 1 BEKJ kann ohne anderslautendes vorgängiges Ersuchen der Absenderin oder des Absenders abgesehen werden, wenn:
a. das Dokument im Verfahren nicht nach Artikel 30 Absatz 2 BEKJ benötigt wird; und
b. dem physischen Exemplar kein eigenständiger Beweiswert zukommt oder ihm in digitalisierter Form derselbe Beweiswert zukommt.
[2] Dies gilt namentlich für reine Mitteilungen, Ausdrucke elektronisch erstellter Dokumente, Fotokopien und Beilagen, deren Originale bei der Absenderin oder dem Absender verbleiben.
[3] Vorbehalten bleibt die Rückbehaltung oder Rücksendung von Dokumenten, die forensisch relevante Spuren enthalten können, Urkundencharakter haben oder nach dem anwendbaren Prozessrecht im Original benötigt werden.

21.2 Begründung

Die Justizverwaltungsleitung hält zur Begründung des Anliegens Folgendes fest: Werde das BEKJ (Art. 30 Abs. 1) zu eng ausgelegt, würden mit einem Gesetz, mit dem eigentlich der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es bisher nicht gegeben habe. Gerade in Strafverfahren würden grosse Mengen physischer Anzeigen, Beilagen und Mitteilungen eingehen. Eine pauschale Rücksendepflicht würde Porti, Versandarbeit und Verwaltungslast schaffen, ohne verfahrensrechtlichen Mehrwert zu bringen. Zu unterscheiden wäre dabei zwischen blosser Mitteilung bzw. Kopie und Papierstücken mit eigenständigem Beweiswert, etwa Originalurkunden, handschriftlich unterzeichnete Dokumente, Unterlagen mit Siegel, Fingerabdrücke, DNA-Spuren oder sonstigen forensischen Merkmalen.

Art. 30 Abs. 1 BEKJ enthält zwar keine Delegation, auf Verordnungsstufe Ausnahmen von der Rücksendungspflicht für gewisse Dokumente vorzusehen. Laut Ziff. 2.6 des Erläuternden Berichts haben Sie aus diesem Grund in der VEKJ auf solche Ausnahmen verzichtet. Im Licht der Ausführungen der Justizverwaltungsleitung bitten wir Sie dennoch, nochmals zu prüfen, ob nicht Raum besteht für eine Regelung, damit nicht sämtliche eingereichten Dokumente unabhängig von ihrem Inhalt nach der Digitalisierung zurückgeschickt werden müssen.

Zur Begründung im Erläuternden Bericht schlägt die Justizverwaltungsleitung folgende Formulierung vor:
«Art. 30 BEKJ ist so zu verstehen, dass physisch eingereichte Dokumente nicht unabhängig von ihrem verfahrensrechtlichen Gehalt zwingend zurückzusenden sind. Von einer Rücksendung kann insbesondere bei reinen Mitteilungen, Ausdrucken elektronisch erstellter Dokumente und Fotokopien abgesehen werden, wenn die Absenderin oder der Absender keinen Rückversand verlangt und dem physischen Exemplar kein eigenständiger Beweiswert zukommt. Vorbehalten bleiben Dokumente mit Urkundencharakter oder möglichen forensischen Spuren.»

22.1 Antrag zu Art. 23

Die Justizverwaltungsleitung regt an, Buchstabe b sei zu streichen.

22.2 Begründung

Die Anforderungen der ZPO und der StPO gehen nach Auffassung der Justizverwaltungsleitung nicht so weit, als dass in der digitalen Umsetzung ein synchronisierter Zeitstempel, wie in Buchstabe b erwähnt, notwendig wäre. Zudem sollte Art. 23 dahingehend ergänzt werden, dass die elektronische Weitergabe von Dokumenten durch die Mutation von Zugriffsrechten auf eine gemeinsame Datenbank zulässig ist.

23.1 Anträge zu Art. 24

23.1.1

Die Justizverwaltungsleitung regt an, die Bedingungen von Art. 24 seien an diejenigen von Art. 23 anzugleichen.

23.1.2

Die Justizverwaltungsleitung regt an, Art. 24 sei nicht nur auf die Übermittlung von Dokumenten zu beschränken, sondern auf verfahrensbezogene Daten und fachapplikationsbasierte Schnittstellen zu erweitern.

23.2 Begründung

Zur Begründung ihres Anliegens hält die Justizverwaltungsleitung Folgendes fest: Es sei nicht ersichtlich, weshalb Art. 24 strengere Voraussetzungen als Art. 23 setze.

Weiter sollte Art. 24 nicht nur auf die Übermittlung von Dokumenten beschränkt sein, sondern auch auf verfahrensbezogene Daten und fachapplikationsbasierte Schnittstellen erweitert werden. Denkbar sei auch, die Übermittlung von verfahrensbezogenen Daten und fachapplikationsbasierten Schnittstellen in einer separaten, aber gleichwertigen Bestimmung zu regeln. Dies sei erforderlich, weil der Austausch zwischen der Staatsanwaltschaft und der Polizei auch häufig strukturierte Daten, Statusmeldungen, Aufträge, Metadaten, Aktenstrukturen oder Zugriffsrechte und nicht nur PDF-Dokumente beinhalte. Aus Sicht von Chain of Custody, Datenschutz und Interoperabilität brauche es funktional gleichwertige Nachvollziehbarkeit, aber nicht zwingend dieselbe Logik wie bei dateibasierten Plattformübermittlungen.

24.1 Antrag zu Art. 26

Die Justizverwaltungsleitung regt an, Art. 26 sei im Sinne der untenstehenden Begründung abzuändern und zu ergänzen

24.2 Begründung

Für die Justiz ist die Unterzeichnung von Protokollen zentral. Auch bei audiovisueller Aufzeichnung dokumentiere das Verfahrens- bzw. das Rahmenprotokoll zusammen mit der Aufzeich-

nung die Verfahrenshandlung und müsse von den Beteiligten bestätigt werden. Die blosse Aufzählung von Datenkanälen wie Strichbeschaffenheit, Druck, Bewegungsfluss, Bewegungsrichtung und Zeitpunkt genügen aus Sicht der Justizverwaltungsleitung nicht. Entscheidend sei Mindestqualität, Prüfbarkeit, Integritätsschutz, Bindung an das konkrete Protokoll und Interoperabilität zwischen Fachapplikationen und Signaturdiensten. Beschaffungs- und Implementierungsrisiken liessen sich vermeiden, wenn die Verordnung bzw. die technische Konkretisierung Mindestanforderungen festlege und die Orientierung an ISO/IEC 19794-11 ausdrücklich zulasse, ohne damit alle fachlichen Qualitätsfragen als erledigt zu betrachten.

Art. 26 sollte nach Auffassung der Justizverwaltungsleitung nach folgenden Grundsätzen ausgestaltet werden:
Die audiovisuelle Aufzeichnung einer Einvernahme oder einer anderen Verfahrenshandlung ersetze das gesetzlich vorgeschriebene Verfahrens- beziehungsweise Rahmenprotokoll nicht. Das Protokoll dokumentiere den Ablauf, die Beteiligten, die Belehrungen, Anträge, Entscheide und weiteren verfahrensrelevanten Rahmenumstände und sei von den Beteiligten zu bestätigen, soweit das Verfahrensrecht dies vorsehe. Die elektronische Bestätigung müsse beweissicher mit dem Protokoll verbunden werden. Werden dynamische beziehungsweise biometrische Signaturdaten erhoben, genüge es nicht, die Arten der erfassten Merkmale zu nennen. Festzulegen seien Mindestanforderungen an Erfassungsqualität, zeitliche und räumliche Auflösung, Druckerfassung, Integritätsschutz, Protokollbindung, Verschlüsselung, Prüfbarkeit und Löschung. ISO/IEC 19794-11 könne als Austauschstandard für dynamische Signaturdaten berücksichtigt werden; die konkrete Verfahrens- und Beweisqualität sei zusätzlich zu regeln.

25.1 Antrag für eine zusätzliche Bestimmung für die eindeutige Identifikation der Aktenstücke

Die Justizverwaltungsleitung regt an, die Verordnung sei mit einer zusätzlichen Bestimmung zu ergänzen, welche die eindeutige Identifikation der Aktenstücke regle. Aus systematischen Gründen sollte für diese Bestimmung ein neues Kapitel unter dem Titel: «Eindeutige Identifikation von Aktenstücken» eingefügt werden.

25.2 Begründung

Die Justizverwaltungsleitung führt zur Begründung ihres Anliegens Folgendes aus: Die eindeutige technische Identifikation jedes Aktenstücks sei eine zentrale Voraussetzung für eine verlässliche elektronische Aktenführung. Ein UUID erlaube es, ein Aktenstück über seinen gesamten Lebenszyklus hinweg systemübergreifend eindeutig zu referenzieren, unabhängig davon, ob sich Dateinamen, Dokumenttitel, Aktenverzeichniseinträge, Speicherorte oder technische Ablagestrukturen ändern.

Die Vorgabe diene insbesondere der Nachvollziehbarkeit bei Scanprozessen, bei der Übermittlung zwischen Behörden, bei der Migration bestehender elektronischer Dossiers, bei der Archivierung sowie bei der späteren Wiederverwendung oder erneuten Bereitstellung von Aktenstücken. Sie reduziere das Risiko von Verwechslungen, Dubletten, Medienbrüchen und fehlerhaften Zuordnungen.

Der UUID sei nicht als neue verfahrensrechtliche Aktennummer zu verstehen. Er habe rein technische Identifikationsfunktion und ersetze weder Geschäftsnummern noch Aktenzeichen oder fachliche Dokumentbezeichnungen. Ebenso solle die Bestimmung keine zusätzliche formelle Gültigkeitsvoraussetzung für Aktenstücke schaffen. Fehler bei der Vergabe oder Führung

des Identifikators seien technisch und organisatorisch zu korrigieren, sollen aber nicht ohne Weiteres die rechtliche Verwertbarkeit eines Aktenstücks in Frage stellen.
Besonders wichtig sei die Regelung für bestehende digitale Dossiers und Legacy-Scans. Bereits heute würden in der Praxis trotz Papierprimat z.T. vollständige elektronische Dossiers geführt. Diese müssten nach Inkrafttreten des BEKJ ohne unnötige Neudigitalisierung oder manuelle Neuerfassung als vollwertige digitale Dossiers weiterverwendet werden können. Die nachträgliche Vergabe eines UUID schaffe hierfür eine einfache, robuste und nachvollziehbare technische Brücke.

Zwar enthält Art. 30 Abs. 1 BEKJ keine Delegation, auf Verordnungsstufe die vorgeschlagene technische Identifikation der Akten zu regeln. Thematisch gehört dies zur Pflicht zur elektronischen Aktenführung, wie sie z.B. in Art. 128b Abs. 1 ZPO festgehalten ist. Wir bitten Sie im Licht der Ausführungen der Justizverwaltungsleitung dennoch zu prüfen, ob nicht Raum besteht für eine Regelung zur technischen Identifikation der Akten.

26.1 Antrag für Ausführungsbestimmungen zu Art. 18 Abs. 2 BEKJ

Es seien Ausführungsbestimmungen zu Art. 18 Abs. 2 BEKJ in die VEKJ aufzunehmen, in denen geregelt wird, auf welche Verfahren sich der Eintrag in das Verzeichnis der Plattform bezieht.

26.2 Begründung

In dem erst vom Parlament eingefügten Abs. 2 von Art. 18 BEKJ ist unklar, auf welche Verfahren sich der Eintrag in das Verzeichnis der Plattform bezieht. Ist ein *konkretes, hängiges* Verfahren gemeint, in dem der Eintragende freiwillig über die Plattform kommunizieren will, oder sind *sämtliche künftige, noch nicht hängige* Verfahren gemeint? Die Frage ist auch, *vor welchen Instanzen* diese Verfahren ablaufen werden: Nur vor der Instanz, bei der ein konkretes Verfahren hängig ist, oder auch vor der nächsthöheren Instanz, bei der möglicherweise ein Rechtsmittel erhoben wird? Oder sind nur sämtliche (auch künftige) Verfahren in einem *bestimmten Rechtsgebiet* betroffen? Es wird selten der Fall sein, dass ein Benutzer im Voraus weiss, in welchen Verfahren er beteiligt sein wird. Es ist unwahrscheinlich, dass Benutzerinnen bzw. Benutzer sich auf Vorrat auf einer Plattform registrieren, die sie möglicherweise nie verwenden werden.

Unklar ist weiter das Verhältnis von Art. 18 Abs. 2 BEKJ zu nArt. 11b Abs. 2 und nArt. 47b VwVG sowie den analogen Bestimmungen in weiteren Verfahrensgesetzen wie dem BGG, der ZPO und der StPO. Klar dürfte bloss sein, dass z.B. Art. 47a VwVG der *Widerruf* der Meldung nach Art. 11b Abs. 2 VwVG ist. Nicht geklärt ist indessen, in welchem Verhältnis Art. 11b Abs. 2 VwVG zu Art. 18 Abs. 2 BEKJ steht. Wir regen deshalb an, die erwähnten Regelungen in der Verordnung zu verdeutlichen. Es fehlt zwar hinsichtlich Art. 18 Abs. 2 BEKJ eine ausdrückliche Delegation an den Bundesrat, dennoch bitten wir Sie zu prüfen, ob nicht doch Raum besteht für die beantragte Regelung.

3. Weiteres

Sie ersuchen uns, Stellung zu nehmen zum Zeitpunkt der abschliessenden Inkraftsetzung des BEKJ. Als frühestmöglicher Zeitpunkt für die Inkraftsetzung des BEKJ und damit auch der VEKJ

geben Sie den 1. Januar 2027 an, wobei gemäss neuster Kommunikation der 1. Juli 2027 geplant ist. Wir halten den 1. Januar 2027 aus folgenden Gründen für unrealistisch:

Gemäss Ziff. 1 des Erläuternden Bericht zur VEKJ (Ausgangslage) muss die Gründung der Körperschaft justitia.swiss (formelles Gründungsdatum) zwingend *vor* dem Inkrafttreten der restlichen Bestimmungen des BEKJ erfolgen. Die Gründungsversammlung kann bereits vorher erfolgen; nach unseren Informationen soll dies im November 2026 der Fall sein. Der Gedanke dahinter ist, dass mit dem vollständigen Inkrafttreten des BEKJ die Körperschaft bereits funktionsfähig sein muss und ihre Arbeit aufnehmen kann. In Ziff. 1 ist denn auch als weitere Voraussetzung für das Inkrafttreten der restlichen Bestimmungen des BEKJ erwähnt, dass die Bewilligung für die Plattform justitia.swiss vorliegt und diese in Betrieb genommen werden kann.

Aus Sicht der Kantone ist – nebst der Erreichbarkeit sämtlicher vom BEKJ erfassten kantonalen Gerichte auf einer der Plattformen (Art. 37 Abs. 1 Satz 3 BEKJ) – noch ein weiterer Punkt zu beachten: Es gibt Kantone, in denen die Ratifikation der Vereinbarung justitia.swiss vom Parlament genehmigt werden muss. Dazu gehört der Kanton Bern, dessen Beitritt zur Vereinbarung geplant ist. Hier läuft ab dem Beschluss des Parlaments (Grosser Rat) zum Beitritt, der voraussichtlich im September 2026 erfolgt, eine 3-monatige Referendumsfrist. Diese läuft voraussichtlich knapp vor Jahresende 2026 oder sogar erst nach dem 1. Januar 2027 ab. Dies hat zur Folge, dass der Beschluss des Parlaments (Grossratsbeschluss) frühestens am 1. März 2027 in Kraft treten kann. Dieser sollte wiederum koordiniert sein mit dem formellen Gründungsdatum der Körperschaft justitia.swiss. Unter diesen Umständen ist es aus unserer Sicht undenkbar, die abschliessende Inkraftsetzung des BEKJ auf den 1. Januar 2027 festzulegen. Realistisch dürfte somit frühestens der 1. Juli 2027 sein.

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates

Pierre Alain Schnegg
Regierungspräsident

Christoph Auer
Staatsschreiber

Verteiler
- Bau- und Verkehrsdirektion
- Wirtschafts-, Energie- und Umweltdirektion
- Bildungs- und Kulturdirektion
- Gesundheits-, Sozial- und Integrationsdirektion
- Staatskanzlei
- Finanzdirektion
- Datenschutzaufsichtsstelle (DSA)
- Justizverwaltungsleitung
- Sicherheitsdirektion
- Direktion für Inneres und Justiz

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Route des Arsenaux 41, 1700 Fribourg

T +41 26 305 10 40
www.fr.ch/ce

Conseil d'Etat
Route des Arsenaux 41, 1700 Fribourg

PAR COURRIEL

Département fédéral de justice et police DFJP
Palais fédéral ouest
3003 Berne

Courriel : cornelia.perler@bj.admin.ch

Fribourg, le 9 juin 2026

2026-567
Ordonnance sur la communication électronique dans les procédure judiciaires et administratives régies par le droit fédéral (OCEP) - Procédure de consultation

Monsieur le Conseiller fédéral,

La procédure de consultation citée en titre a retenu toute notre attention et nous vous remercions de nous avoir consultés.

Nous saluons le projet de cette future ordonnance qui permettra d'établir et donner un cadre juridique précis concernant la communication électronique dans les procédures judiciaires et administratives.

À la suite de la consultation des autorités judiciaires de notre canton, nous tenons à formuler les observations et craintes suivantes concernant certaines dispositions de l'OCEP ainsi que de la LPCJ.

> **Art. 1 – Champ d'application**

Les offices des poursuites et faillites devront également transmettre des documents par la voie électronique. Il est ainsi essentiel que cette ordonnance ainsi que les dispositions y relatives ne puissent pas primer sur la législation actuelle. En effet et en application des art. 15 OAOF, lesdits offices ont l'obligation de pourvoir à la conservation des pièces comptables des sociétés dont ils assument la liquidation. Ces documents représentent un volume important et ne peuvent être transmis par voie électronique. Dans ce sens, il conviendrait de préciser l'art. 1 al. 3 en indiquant

« *les dispositions de droit fédéral sont réservées et priment sur celles de la présente ordonnance* ».

Cette modification permettrait aux offices de continuer à avoir la possibilité de refuser la transmission de renseignements ou documents par voie électronique concernant certaines requêtes faites par des tiers, si la situation l'exige.

> **Art. 4 al. 2, 3 et 4 OCEP – Format des documents**

Afin d'éviter aux autorités judiciaires du travail supplémentaire en devant faire des conversions de documents reçus ou de demander à l'expéditeur qu'il fasse une conversion dans un format PDF ou PDF/A, l'alinéa 2 devrait être libellé comme suit :

> *[2] Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine.*

Notre expérience avec la solution Proofbox (e-justice) met en évidence la complexité de la gestion des formats de documents, notamment en raison de la nécessité de convertir ceux qui ne répondent pas aux standards prédéfinis, avec un délai de conversion incombant à la partie émettrice. Dès lors que la liste des formats doit demeurer évolutive au gré des avancées technologiques, il apparaît inopportun de l'inscrire dans une ordonnance, une annexe offrant la flexibilité requise. Enfin, l'attribution de la conversion à l'émetteur du document constitue une approche pragmatique, conforme à la pratique actuelle.

À titre de proposition, les alinéas 3 et 4 pourraient être formulés comme suit :

> *[3] Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour qu'elle puisse la transmettre dans un format défini par l'autorité.*
>
> *[4] Le DFJP définit les formats de fichiers à transmettre via la plateforme.*

L'alinéa 5 devrait quant à lui être abrogé.

> **Art. 5 al. 2 let. b OCEP – Nom de l'expéditeur**

La disposition proposée exige que les quittances d'envoi des documents électroniques mentionnent en particulier "*le nom de l'expéditeur*, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit". Cette formulation, qui laisse entendre que le nom de la personne physique, donc du collaborateur, qui effectue l'envoi au nom de l'autorité judiciaire pour qui il travaille, figurera sur la quittance, ne devrait pas trouver application aux autorités judiciaires. Afin de protéger les collaborateurs, en particulier administratifs, qui se chargent en règle générale des envois, il nous paraît important que leur nom ne soit pas mentionné sur les quittances. En outre, à l'instar de ce que prévoit l'art. 9 OCEP pour les données qui doivent figurer dans les profils, il convient de faire une distinction entre les autorités judiciaires et les autres utilisateurs de la plateforme. Les autorités doivent ainsi mentionner dans leur profil le nom de l'autorité, l'adresse postale et le nom du cachet et il est cohérent que la quittance d'envoi reflète ces données institutionnelles et non l'identité du collaborateur chargé de l'opération matérielle. Afin de clarifier ce point à l'attention des exploitants de la plateforme et de ses utilisateurs, il conviendrait de prévoir une disposition spéciale pour les autorités judiciaires, qui pourrait avoir la teneur suivante : « *le nom de l'autorité judiciaire expéditrice et son adresse sur la plateforme* ».

> **Art. 6 OCEP – Apposition d'un cachet par l'autorité expéditrice**

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Par ailleurs l'obligation d'apposer un cachet aux autorités qui dirigent la procédure ainsi qu'aux autorités qui y participent est en contradiction avec le concept technique de la plateforme centralisée.

> **Art. 7 al. 1 et 2 OCEP – Apposition d'un cachet par la plateforme**

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la quittance, jamais le document transmis. Dans le cas de la plateforme centralisée, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait ainsi être libellé comme suit :

> *[1] Lorsque des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. L'alinéa. 2 doit donc être supprimé.

> **Art. 9 al. 2 et 3 let. a et b OCEP – Profils**

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, car une autorité peut disposer de plusieurs sites. L'alinéa de cette disposition doit être adaptée en conséquence :

> *[2] Les profils des autorités comprennent au moins les données suivantes :*
>
> *a.le nom de l'autorité ;*
> *b. le nom du cachet*

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et administratif. Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs doit être considéré comme critique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques. Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique. Il convient donc de renoncer à l'adresse postale également pour les organisations.

L'alinéa 3 let. a et b devrait avoir la teneur suivante :

> *[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :*
>
> *a. pour les personnes physiques : le prénom, le nom, et la date de naissance ;*
> *b. pour les organisations : le nom de l'organisation ou de l'entreprise.*

> **Art. 16 – Répartition de l'émoluments**

Nous nous opposons fermement à la clé de répartition prévue à cette disposition. Les recommandations Justitia 4.0 estiment que les coûts annuels nécessaires à l'exploitation et au développement ultérieur de la plateforme centralisée se situeront entre 10 et 12 millions de francs ; puisque le projet prévoit une participation de la Confédération à raison de 10 %, les cantons devront supporter les 90 % restants, partant des frais de l'ordre de 9 000 000 à 10 800 000 francs, selon une répartition proportionnelle à leur population. A ce stade, il convient de rappeler l'entrée en vigueur de l'ordonnance sur le financement de la surveillance de la correspondance par poste et télécommunication (RS 780.115.1), qui prévoyait une répartition Confédération/canton de 25 %/75 %. Nous avions alors revendiqué une augmentation de la part de la Confédération, en vain ; la facture finale a ensuite entraîné une explosion des coûts à charge du canton. Même si comparaison n'est pas raison, nous nous devons de nous élever contre cette répartition 10 %/90 % dans le projet OCEP, répartition qui se base sur le seul nombre de procédures liquidées par chaque autorité (cf. rapport page 27) ; il est en effet réducteur de vouloir attribuer la même valeur entre les dossiers d'envergure conduits par le MPC et les très nombreux dossiers de masse sous la compétence des MP cantonaux. Les échanges électroniques que suppose la gestion de ces derniers dossiers ne sont en effet en aucun cas comparables avec ceux du MPC. Il est dès lors faux de vouloir procéder par une comparaison du nombre de dossiers pour fonder la participation financière des cantons par rapport à la Confédération. Il s'ensuit que la répartition de la participation financière Confédération/cantons doit absolument être revue, par une augmentation significative de la part mis à la charge de la Confédération.

> **Art. 22 OCEP – Numérisation de documents physiques**

L'obligation pour les autorités de restituer les documents prescrits à l'art. 30 LPCJ constitue une charge de travail supplémentaire et engendrera un coût, notamment en matière de frais postaux. L'introduction d'un nouvel art. 22a OCEP nous paraît judicieuse. Cela étant, indépendamment d'une demande en ce sens de la part de l'expéditeur, la destruction, cas échéant, impliquera quoi qu'il advienne une charge (personnelle et financière), mais dans une moindre mesure.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. La résolution de 300 dpi semble judicieuse. Il convient de noter qu'avec une résolution de 300 dpi, la taille du fichier est quatre fois supérieure à celle obtenue avec une résolution de 150 dpi.

> **Art. 22*a* OCEP – Renvoi de documents physiques (proposition)**

Tel que formulé, le texte de l'art. 30 al. 1 LPCJ laisse la porte ouverte à une interprétation extensive qui aurait pour conséquence que les autorités judiciaires devraient systématiquement retourner à l'expéditeur tous les documents physiques reçus, à savoir en particulier tous les mémoires de demande, de recours, de réponse, etc., destinés et établis pour l'autorité judiciaire. Or, une telle interprétation est en contradiction totale non seulement avec la digitalisation, mais également avec la pratique actuelle des tribunaux. Il ne viendrait en effet à l'idée de personne, aujourd'hui, de retourner aux justiciables l'ensemble de leurs envois. Cette faculté doit tout au plus être réservée au renvoi de documents originaux produits dans le cadre de certaines procédures (testament, acte notarié, plans originaux, etc.) parce qu'ils présentent une valeur probante particulière. La disposition légale précitée ne serait en outre pas comprise par les

justiciables et engendrerait un travail et des coûts postaux énormes. En effet, faut-il rappeler que seuls les avocats seront contraints de communiquer par le biais de la plateforme avec les autorités judiciaires. Or, de très nombreuses procédures sont menées par les justiciables eux-mêmes qui continueront dès lors pour l'essentiel à utiliser le papier et la voie postale pour communiquer avec les autorités judiciaires.

Il faut par conséquent impérativement préciser dans l'ordonnance que l'art. 30 al. 1 LPCJ doit être interprété restrictivement. Contrairement à l'Office fédéral de la justice, nous pensons que la LPCJ permet une telle interprétation. La disposition topique pourrait avoir la teneur suivante :

Art. 22a – Renvoi de documents physiques

Les documents physiques établis à destination de l'autorité judiciaire (courriers, mémoires, bordereaux de pièces) ne sont renvoyés à leur expéditeur que si celui-ci en a fait expressément la demande au moment de leur dépôt ou s'il s'agit de documents originaux.

Le principe d'une digitalisation est de privilégier le digital, voire basculer des pratiques de travail réalisées sur du papier vers le digital. Également, la simplification des processus de travail est au cœur des bénéfices qui doivent être constamment recherchés. Dès lors, imposer encore des manipulations administratives avec l'usage du papier va à l'encontre de la digitalisation. Si cette pratique est maintenue, la diminution de la charge de travail ne sera pas atteinte ; un risque de complexification des tâches pourrait même naître.

> **Signature si le document est envoyé sur papier** (art. 133 let. h, 235 al. 1 let. f et 238 let. h CPC, art. 80 al. 2, 201 al. 2 let. h et 353 al. 1 let. k CPP [pas encore en vigueur])

La LPCJ modifie certaines dispositions du CPC et du CPP et, ce faisant, introduit une précision aux articles susmentionnés dont l'interprétation pourrait donner lieu à discussion, de sorte qu'il se justifie de la clarifier d'emblée. Les six dispositions mentionnées précisent chacune qu'un acte déterminé doit contenir "la signature" du tribunal, du préposé au procès-verbal, de la personne qui l'a décerné, de la personne qui a établi l'ordonnance, si le document (citation, procès-verbal, décision, mandat de comparution, ordonnance pénale) a été envoyé sur papier.

Selon la jurisprudence fédérale, les dispositions précitées du CPP signifient que les actes en question ne sont valides que lorsqu'ils sont munis de la signature manuscrite de leur auteur formel, procureur ou juge (voir ATF 148 IV 445 consid. 1.3.2; arrêt TF 6B_199/2024 du 28 mai 2024 consid. 1.1 et les références) ou signés en son absence par un collègue (arrêt TF 7B_164/2022 du 14 août 2023 consid. 3). Le Tribunal fédéral a toutefois précisé qu'il suffisait qu'un document comportant une signature valable figure au dossier judiciaire, de sorte que l'envoi de documents comportant des signatures photocopiées ou facsimile était acceptable (voir arrêt TF 6B_9/2024 du 30 avril 2025 consid. 1.3.4 *in fine*).

Il découle de ce qui précède que, dans l'univers du dossier judiciaire sur papier, une signature manuscrite sur l'acte qui reste au dossier judiciaire est suffisante pour attester que l'auteur de l'acte en a pris la responsabilité. Il doit en aller de même dans l'univers du dossier judiciaire électronique. Dès lors que l'auteur formel de l'acte en a pris la responsabilité en le validant électroniquement, il doit être possible d'en faire parvenir aux destinataires un exemplaire sur papier qui mentionne expressément que l'original électronique a été dûment "signé", au sens électronique du terme, c'est-à dire validé et qu'il peut être consulté au siège de l'autorité.

Or, il ressort du commentaire accompagnant l'avant-projet de l'ordonnance que l'Office fédéral de la justice part de la prémisse que tous les documents envoyés sur papier devront être munis d'une signature manuscrite. Si nous partageons l'appréciation selon laquelle une "signature" du document original est nécessaire, nous estimons toutefois qu'une validation électronique est équivalente à cet égard.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr être effectuée au moyen d'un exemplaire sur papier de l'original (désormais établi par voie électronique), original qui reste dans le dossier judiciaire électronique. Si le destinataire a des doutes quant à l'authenticité de la décision et/ou de sa validation par son auteur formel, il peut à tout moment, comme aujourd'hui déjà, se faire présenter l'original (électronique) au siège de l'autorité (voir arrêt TF 4A_455/2024 du 27 janvier 2025 consid. 2). La solution proposée présente en outre l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant.

Une solution intermédiaire consisterait à prévoir une validation électronique de l'auteur de l'acte (en plus du cachet de l'autorité), afin de satisfaire à l'exigence de la "signature" de l'auteur formel de l'acte utilisée dans les lois de procédure, signature permettant d'attester que cette personne a bien pris la responsabilité dudit acte.

Nous proposons par conséquent d'introduire dans l'ordonnance la disposition suivante :

> [1] *Les autorités judiciaires qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents qu'elles envoient par voie électronique. En cas d'envoi du document sur papier, celui-ci mentionne expressément que l'original électronique comporte ce cachet et peut être consulté au siège de l'autorité.*
>
> [2] *Lorsque le droit procédural applicable exige la signature d'une personne déterminée, la validation électronique par cette personne est mentionnée expressément sur le document envoyé par voie électronique ou sur papier.*

En vous remerciant de nous avoir consultés, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre considération distinguée.

Au nom du Conseil d'Etat :

Philippe Demierre, Président

CONSEIL D'ETAT CANTON DE FRIBOURG

Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Copie

—

à la Direction de Sécurité, de la Justice et du sport (DSJS), pour elle et le Service de la justice ;
à la Chancellerie d'Etat.

RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 1er juillet 2026

Le Conseil d'Etat

2854-2026

Département fédéral de justice et police
Monsieur Beat Jans
Conseiller fédéral
Palais Fédéral Ouest
3003 Berne

Concerne : consultation fédérale relative au projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,

Notre Conseil a bien reçu votre courrier du 13 mars 2026, par lequel vous avez invité les Gouvernements cantonaux à se prononcer dans le cadre de la procédure de consultation citée en marge.

Après en avoir pris connaissance avec intérêt et attention, nous vous prions de trouver, dans le document annexé à la présente, la prise de position du Conseil d'État, établie en concertation avec le Pouvoir judiciaire.

En vous remerciant de nous avoir consultés, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre haute considération .

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti-El Zayadi

La présidente :

Anne Hiltpold

Annexe mentionnée

Copie à (*format Word et pdf*) : cornelia.perler@bj.admin.ch

Annexe

Consultation fédérale relative à l'Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Prise de position du Conseil d'État de la République et canton de Genève

---

I. Introduction

Le Conseil d'État attire en particulier votre attention sur ses observations en lien avec les articles 23 et 24 du projet, résumées ici en préambule.

- Les autorités judiciaires et les gouvernements cantonaux sont intervenus, durant les travaux parlementaires portant sur la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ) du 20 décembre 2024, pour que soit prévue la possibilité, pour les autorités chargées de diriger la procédure, de communiquer, dans certains cas, sous forme électronique mais sans recourir à l'une des plateformes au sens de la loi. Il s'agissait d'éviter que les autorités judiciaires ne doivent utiliser une plateforme lorsqu'elles communiquent à une autre autorité des documents ou instructions sans que ladite communication n'ait d'effet pour les parties à la procédure. Étaient notamment visées : la transmission du dossier judiciaire d'un tribunal de première instance au tribunal cantonal, la transmission du rapport de police au ministère public, la communication d'instructions du ministère public à la police ou encore la communication de documents d'une autorité administrative ou d'un service administratif à l'autorité judiciaire.

  Le Parlement fédéral a fait droit à cette demande et introduit la possibilité pour les autorités judiciaires de procéder à des communications électroniques sans recourir à la plateforme, sur un plan intracantonal (procédures civiles et pénales) et sur un plan intercantonal (procédures pénales). De telles communications électroniques doivent ainsi pouvoir intervenir sans passer par une plateforme au sens de la LPCJ, par exemple par le biais d'un interfaçage des systèmes d'information à l'intérieur d'un canton (notamment entre la police et le ministère public) ou encore par la modification ponctuelle des droits d'accès dans un système d'information commun (par exemple pour communiquer un dossier du tribunal de première instance au tribunal supérieur).

  Les articles 23 et 24 du projet d'ordonnance, censés concrétiser cette possibilité introduite durant les travaux parlementaires à la demande des autorités judiciaires, doivent impérativement être revus. Leur formulation et leur articulation sont en l'état incompréhensibles, de même que leur champ d'application concret. Ils posent en outre des exigences et conditions telles qu'ils enlèvent tout intérêt au mode alternatif de communication électronique introduit dans la LPCJ.

  Au vu de la technicité de cette question, le Conseil d'État recommande que l'office fédéral de la justice remette l'ouvrage sur le métier en concertation avec le groupe d'experts du projet Justitia 4.0, notamment composé de magistrats expérimentés pouvant expliquer les enjeux en présence et apporter un éclairage indispensable.

- La plateforme justitia.swiss propose en principe la communication du document lui-même. Elle teste toutefois avec le canton de Bâle-ville une alternative avec le stockage décentralisé des documents dans les systèmes d'information de ce canton, la plateforme y donnant simplement accès. Dans cette variante, le document ne transite pas par la plateforme. Le canton de Genève pourrait être intéressé par ce mode de fonctionnement mais s'interroge sur les éléments suivants : a) la plateforme ne peut vérifier si les documents sont munis d'un cachet électronique, b) elle ne peut vérifier que les documents sont exempts de logiciel malveillant et c) elle peut émettre une quittance de consultation sans pouvoir vérifier que le document existe ou est accessible. Il paraît important que ces questions soient vérifiées et traitées pour les cantons souhaitant adopter le mode décentralisé.

- Le Conseil d'État souligne en outre l'importance des observations formulées en lien avec l'article 4, alinéa 2, ainsi qu'avec deux articles nouveaux qu'il est proposé d'introduire, soit les articles 22a et 22b.

II. Commentaires d'articles

Concernant le préambule du projet d'ordonnance

Le projet d'ordonnance omet délibérément de citer les articles qui confèrent au Conseil fédéral la compétence de réglementer le format des documents transmis par voie électronique. Le rapport explicatif précise que, « *pour conserver une vue d'ensemble* », le préambule ne mentionne que les dispositions des lois de procédure qui traitent de la communication en dehors des plateformes de la LPCJ. Le canton de Genève estime qu'il est préférable de mentionner toutes les normes de délégation contenues dans les lois de procédure. Cela vaut en particulier pour les articles qui confèrent au Conseil fédéral la compétence de définir les formats. Ces dispositions devraient donc logiquement être également mentionnées dans le préambule, qui devrait ainsi être libellé comme suit:

> *vu la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ),*
> *vu l'art. 6a al. 2, 21a al. 2 et 34 al. 1bis de la loi du 20 décembre 1968 sur la procédure administrative du 20 décembre 1968 (PA),*
> *vu l'art. 38e de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF),*
> *vu les art. 128b al. 3 et 128c al. 2 et 128e du code de procédure civile du 19 décembre 2008 (CPC),*
> *vu les art. 33a al. 4, 33b, 33c al. 2 et 34 al. 3 de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),*
> *vu les art. 76a al. 2, 103b al. 3, et 103c al. 2 et 103e du code de procédure pénale du 5 octobre 2007 (CPP),*
> *vu l'art. 2e de la loi fédérale du 23 décembre 2011 sur la protection extraprocédurale des témoins (Ltém),*
> *vu l'art. 31f de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA),*
> *vu les art. 8c al. 3, et 8d al. 2 et 8f de la loi du 23 mars 2007 sur l'aide aux victimes (LAVI),*
> *vu les art. 37d et 38a al. 2 de la procédure pénale militaire du 23 mars 1979 (PPM),*

Ad article 1

Selon notre interprétation, l'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral, étant rappelé que les procédures administratives cantonales sont exclues du champ d'application de la LPCJ.

L'alinéa 3 peut être supprimé.

Ad article 2 Conditions applicables aux plateformes

Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre c, doit être fixée dans une annexe à l'ordonnance soumise à la présente consultation, ou dans une ordonnance du département fédéral de justice et police. Le Conseil d'État considère en effet que l'OCEP n'est pas le bon niveau normatif pour régler cette question. Elle doit en revanche contenir une norme de délégation sur ce point.

La lettre d de l'alinéa premier de cette disposition n'a pas sa place à cet endroit. Elle définit en effet une fonctionnalité, qui doit être réglementée dans la section 3 de l'ordonnance. Par ailleurs, la formulation est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport explicatif, à la page 11, la fonction de suppression a pour effet d'effacer l'autorisation individuelle accordée mais pas le document lui-même. Il convient en outre, s'agissant de la fonction de suppression, de faire la distinction entre les autorités et les autres utilisateurs.

Ad article 4 **Format des documents**

Remarque générale

Le projet utilise, à l'instar de la LPCJ, le terme « document » plutôt que celui de « fichier » (cf. message LPCJ, p. 20), au motif que le terme « fichier » est un terme trop technique pour être utilisé dans la loi. Le terme « fichier » doit en revanche être utilisé dans l'ordonnance, qui qualifie d'un point de vue technique les annexes transmises.

Ad alinéa 2

Le Conseil d'État souligne que l'alinéa 2 de l'article 4 doit impérativement être modifié.

En effet, dans la très grande majorité des cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Pour ce motif, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocates et avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. En soumettant leurs pièces jointes en format PDF, les parties évitent leur conversion par les autorités judiciaires en format PDF et toutes les parties disposent du même document.

La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si en règle générale les documents sont disponibles au format PDF, cela permettra un traitement rapide par les avocates et avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocates et avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers. Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. Elles devraient en outre le convertir pour pouvoir utiliser pleinement les applications permettant de travailler avec un dossier judiciaire électronique. Les avocates et avocats ou les autorités administratives devraient faire de même. Il en découlerait un surcroît de travail important et, partant, une perte d'efficience, sans pour autant qu'il n'y ait de valeur ajoutée au dépôt du document sous un autre format. Il en découlerait en outre des risques de confusion.

En d'autres termes, il est important de prévoir que les parties et les avocates et avocats doivent en principe produire les annexes en fichier PDF et non en format original. Dans la quasi-totalité des cas, la production du fichier original (par exemple Excel, Word ou PowerPoint) ne présenterait aucune valeur ajoutée et entraverait l'utilisation des applications de travail avec les dossiers judiciaires électroniques. Dans les rares cas où la partie ou l'avocate ou l'avocat estime que le fichier original doit être produit au motif qu'il contient des informations importantes que le fichier PDF ne contiendrait pas, la production du fichier original doit évidemment être possible.

À noter par ailleurs que le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées.

Pour le surplus, même avec une liste élargie de formats acceptables, certains fichiers ne pourront être lus, en raison d'un format moins courant. On peut notamment penser à des enregistrements audio ou vidéo.

Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format ZIP.

Enfin, les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centrale.

Au vu de ce qui précède, le Conseil d'État considère que l'alinéa 2 devrait être libellé comme suit :

> [2] ~~*Les annexes peuvent être remises dans n'importe quel format*~~ *Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine*.

Ad alinéas 3 et 4

Si la sélection de formats de fichiers proposée peut convenir, le niveau normatif est inadéquat. La définition des formats que les autorités chargées de la procédure doivent pouvoir traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP.

La liste des formats de fichiers pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.).

Ces éléments doivent figurer dans une annexe à l'ordonnance.

Les alinéas 3 et 4 devraient donc être libellés comme suit :

> [3] ~~*L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :*~~*Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour la transmettre dans un format défini par l'autorité.*
> ~~*a. documents écrits : PDF, PDF/A ;*~~
> ~~*b. images : BMP, GIF, JPEG, PNG ;*~~
> ~~*c. fichiers audio : MP3, OGG, WAV ;*~~
> ~~*d. fichiers vidéo : AVI, MOV, MKV, MP4 ;*~~
> ~~*e. fichiers d'archives : ZIP, 7z.*~~
> [4] ~~*Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée*~~ *Le DFJP définit les formats de fichiers à transmettre via la plateforme*.
> [5] ~~*L'autorité qui dirige la procédure fixe un délai approprié.*~~

Ad article 5 **Quittances**

Le nom de la personne responsable d'une autorité, au sens de **l'alinéa 2, lettre b**, ne doit pas figurer sur la quittance. Seul le nom de l'autorité doit apparaître.

Un résultat positif lors du contrôle antivirus visé à **l'alinéa 2, lettre d, chiffre 2**, constitue un motif possible de rejet du fichier par la plateforme, mais ce n'est pas le seul. La taille ou le format du fichier peuvent également en être la cause. Nous sommes d'avis que la quittance doit pouvoir faire mention des autres causes de rejet.

L'alinéa 2, lettre d, chiffre 2, précise que les documents qui n'ont pas été transmis suite au résultat de l'analyse de l'antivirus sont mentionnés dans la quittance de réception. Nous considérons que la quittance devrait le cas échéant faire également mention de la valeur de hachage des documents rejetés, pour éviter tout contentieux ultérieur sur la nature du document dont la transmission a échoué. Le chiffre 2 devrait être modifié en conséquence :

> [2] *Les quittances comportent en particulier les données suivantes:*
> *a. le type de quittance ;*
> *b. le nom de l'expéditeur, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit;*
> *c. le nom du destinataire ou de son entreprise et son adresse sur la plateforme;*
> *d. pour la quittance de réception :*
> *1. la liste des documents transmis, leur taille et leur valeur de hachage,*
> *2. la liste des documents qui n'ont pas été transmis, avec indication de leur taille, de leur valeur de hachage et de la raison de la non-transmission,*
> *3. le moment de la transmission à la plateforme ;*

À noter qu'il existe plusieurs algorithmes permettant de calculer la valeur de hachage. Afin de garantir la traçabilité et la validité juridique de cette valeur, l'algorithme utilisé pour son calcul doit être explicitement identifié. Il est proposé d'intégrer une clause de délégation permettant au département de définir et de publier l'algorithme applicable pour le calcul des valeurs de hachage.

Les plateformes permettront à l'avenir de transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car pour des raisons techniques, les fichiers XML ne peuvent ou ne doivent pas forcément être cachetés.

Ad article 6 **Apposition d'un cachet par l'autorité expéditrice**

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure apposera son cachet sur l'un des documents transmis avant leur envoi à la plateforme ; il s'agira généralement de la décision (ordonnance, jugement, arrêt) ou d'une correspondance. La plateforme au contraire apposera un cachet après la transmission à la plateforme, sur la quittance émise sur la base de l'article 5.

L'article 6 règle l'apposition d'un cachet sur les documents par l'autorité dirigeant la procédure avant leur transmission par l'intermédiaire d'une plateforme (art. 22 al. 2 LPCJ). Le projet prévoit que « *lorsqu'une autorité transmet à la plateforme plusieurs documents en même temps, il suffit qu'un de ces documents soit muni d'un cachet et d'un horodatage* », ce qui est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examinée indépendamment de la plateforme.

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit et doit impérativement suffire. Par ailleurs, l'obligation faite aux autorités qui dirigent la procédure et aux autorités qui y participent d'apposer un cachet est en contradiction avec le concept technique de la plateforme centralisée.

Pour diverses fonctionnalités de la plateforme centrale, la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure est essentielle. Ainsi, seules les autorités qui dirigent la procédure pourront procéder à des notifications. Seules les adresses des autorités qui dirigent la procédure seront visibles pour les tiers dans le répertoire public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités participant à la procédure ou communiquant avec l'autorité qui dirige la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations, avocats et particuliers et ce, indépendamment d'une procédure contentieuse. Cela étendrait l'utilisation de la plateforme à toute communication électronique entre autorités, sans aucune base légale. Pour mémoire, l'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires.

Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents. L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision incidente ou le jugement d'une autorité qui dirige la procédure crée des droits et des obligations. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète ou de la plateforme centrale, si le document concerné est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités chargées de la direction de la procédure exercent leurs prérogatives.

Les autorités participant à la procédure ne doivent pas être tenues d'apposer un cachet électronique sur leurs documents. Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante.

Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante à cet effet et n'avait pas cet objectif. L'instauration généralisée d'un cachet électronique entraînerait en outre pour les cantons un effort organisationnel considérable et des coûts importants.

Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond pas au concept de la LPCJ, laquelle ne prescrit aucune fonctionnalité permettant à la plateforme de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre par l'intermédiaire de la plateforme.

Il serait utile de préciser comment les autorités peuvent signer des documents qui, selon la jurisprudence actuelle, doivent porter la signature de leur auteur, comme les expertises (BSK StPO-Heer, art. 187 N 1). Dans le cas des instituts de médecine légale ou de l'Institut fédéral de métrologie METAS, par exemple, ces expertises peuvent tout à fait être réalisées par des autorités ou, à tout le moins, par des « services administratifs ». Dans ces cas, l'identité de l'expert qui établit l'expertise

est déterminante, raison pour laquelle la signature électronique qualifiée (contrairement à ce qui ressort du commentaire de l'art. 22 LPCJ dans le message, FF 2023 679ss, p. 30) devrait probablement continuer à s'appliquer à l'avenir.

Il est important de souligner la différence entre l'envoi et consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents mis à disposition pour la consultation en ligne du dossier.

Ad article 7 Apposition d'un cachet par la plateforme

Remarques générales

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis avant leur envoi à la plateforme ; il s'agit généralement de la décision (ordonnance, jugement ou arrêt) ou de la lettre d'accompagnement (cf. *supra* ad art. 6). La plateforme, en revanche, appose son cachet après la transmission sur la plateforme, sur la quittance de réception émise, qui est régie par l'article 5.

À noter que les conditions applicables en cas d'indisponibilité de la plateforme, notamment celles relatives à la vérification de l'intégrité des documents au moyen des valeurs de hachage, pourraient être utilement définies. L'algorithme de hachage utilisé et les modalités de contrôle et de validation pourraient être précisées, le cas échéant dans une ordonnance du département.

Ad alinéa premier

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la quittance, jamais le document transmis. Dans le cas de la plateforme centrale, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

Ad alinéa 2

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. L'alinéa 2 doit donc être supprimé :

> [2] *~~Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.~~*

Ad article 8 Authentification des utilisateurs

L'authentification par AGOV, conformément à l'alinéa 1, est judicieuse et pertinente. Le Conseil d'État est en effet favorable à une authentification simplifiée pour les collaboratrices et collaborateurs des autorités, ce qui leur permet d'éviter de passer par des étapes supplémentaires de connexion et ainsi de perdre du temps.

L'utilisation éventuelle de services d'authentification supplémentaires dans le cadre de futures plateformes cantonales, conformément à l'alinéa 2, est saluée.

À l'avenir, la plupart des autorités seront reliées à la plateforme par une interface. La disposition proposée à l'alinéa 3 laisse une marge de manœuvre suffisante pour mettre en œuvre de futures solutions techniques.

Le canton de Genève se demande par ailleurs s'il est attendu que l'authentification des membres des autorités judiciaires par leur connexion à leur application métier soit d'un niveau de qualité similaire à celui de la plateforme (AGOV aq300). Si tel était le cas, les autorités judiciaires ne seront vraisemblablement pas en mesure de le faire à bref délai.

Ad article 9 **Profils**

Remarque générale

Le canton de Genève se demande si des mesures sont prévues ou envisagées pour prévenir ou limiter les risques d'usurpation d'identité, permettant notamment la création sans contrôle de compte pour une organisation par ailleurs existante.

Ad alinéa 2

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale car une autorité peut disposer de plusieurs sites. La disposition doit en conséquence être adaptée comme suit :

> *[2] Les profils des autorités comprennent au moins les données suivantes :*
> *a. le nom de l'autorité ;*
> *~~b. l'adresse postale ;~~*
> *b ~~c~~. le nom du cachet.*

Ad alinéa 3, lettre a

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et du droit administratif.

Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. En outre, du point de vue de la protection des données, l'enregistrement de l'adresse privée dans les profils utilisateurs doit être considéré comme problématique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques et de formuler la lettre a de la manière suivante :

> *[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :*
> *a. pour les personnes physiques : le prénom, le nom, la date de naissance ~~et l'adresse postale~~ ;*

Ad alinéa 3, lettre b

Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique. Il convient donc de renoncer à l'adresse postale également pour les organisations.

L'alinéa 3 devrait donc être formulé comme suit :

> [3] *Les profils des autres utilisateurs comprennent au moins les données suivantes :*
> a. *pour les personnes physiques : le prénom, le nom~~,~~ et la date de naissance ~~et l'adresse postale~~ ; …*
> b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Ad alinéa 4

Cet alinéa n'est pas compréhensible, et il y a lieu de le clarifier. On ne comprend en effet pas s'il concerne le profil d'une organisation ou celui d'un particulier.

Le rapport mentionne la personne responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.

Ad article 10 **Interface**

Cet article permet aux utilisatrices et utilisateurs de la plateforme de connecter leurs systèmes à celle-ci par le biais d'une interface et d'octroyer des droits de représentation à leurs collaboratrices et collaborateurs, ce qui se fait par l'intermédiaire d'un utilisateur technique, lequel reçoit un mot de passe numérique (token). La réglementation proposée est donc saluée.

Ad article 11 **Attribution et retrait de droits**

La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait cependant de parler de « confirmation » plutôt que d'« attribution ». Le titre de cette disposition deviendrait ainsi le suivant :

> *Article 11* *Confirmation et retrait de droits*

Ad article 12 **Durée maximale de conservation des documents et des quittances**

Ad alinéa premier

Problématique

L'article 12 du projet d'ordonnance prévoit que les documents et les quittances sont supprimés automatiquement de la plateforme à l'expiration d'un délai de six mois.

Le canton de Genève est favorable à la suppression automatique des documents après un délai raisonnable car la plateforme est conçue comme une « boîte aux lettres », et non comme un moyen de stockage et d'archivage. Le Conseil d'État considère cependant opportun, en ce qui concerne les quittances, de prévoir un délai un peu plus long.

Les quittances sont utiles pour prouver le respect d'un délai ou la prise de connaissance d'un document donné. Il appartient évidemment aux autorités de transférer les quittances dans leurs propres logiciels de gestion d'affaires, en les intégrant à leurs propres systèmes. Cependant, le fait qu'en raison du fonctionnement de la plateforme centralisée, les quittances ne sont pas classées dans les dossiers d'une procédure, par exemple en cas de notification, pourrait conduire à ce que le téléchargement des quittances ne soit pas effectué. Contrairement aux requêtes et aux notifications,

qui peuvent être renvoyées depuis les systèmes sources, les quittances générées par la plateforme elle-même seraient dans ce cas déjà perdues au bout de six mois.

Les quittances peuvent également contenir des données personnelles (telles que les noms des parties à la procédure), ce qui, dans le contexte des procédures judiciaires, peut même en faire des données personnelles particulièrement sensibles. Cependant, ces données, tout comme les pièces du dossier elles-mêmes, bien plus sensibles, sont stockées de manière sécurisée sur la plateforme. À cela s'ajoute le fait que les quittances constituent également de très petites quantités de données, qui ne nécessitent pas de stockage supplémentaire important, même si elles restent disponibles longtemps sur la plateforme.

Proposition

Il est proposé ici de modifier ou de retenir un délai de trois ans, qui correspond au délai pendant lequel la Poste suisse permet d'effectuer des recherches en lien avec le courrier postal.

Par ailleurs, dans la version française, le fait que la suppression est automatique manque dans le libellé de l'alinéa 1, de sorte qu'il convient de l'ajouter.

Le Conseil d'État estime que l'alinéa 1 doit donc être modifié comme suit :

Article 12 Durée maximale de conservation des documents et des quittances

[1] Les documents ~~et les quittances~~ enregistrés sur une plateforme sont automatiquement ~~détruits~~supprimés six mois après leur réception ~~ou leur délivrance~~.
[2] Lorsque des documents peuvent être consultés, l'autorité qui dirige la procédure fixe le délai pendant lequel ils sont disponibles sur la plateforme. Passé ce délai, ils sont automatiquement supprimés ~~détruits~~.
[3] Les quittances sont automatiquement supprimées trois ans après leur délivrance.

Ad alinéa 2

Le canton de Genève est favorable à la solution proposée. Il n'est pas nécessaire de prévoir une prolongation du délai dans l'ordonnance car l'autorité peut ordonner une deuxième consultation du dossier avec les mêmes pièces.

Ad article 13 Sécurité des données

La disposition proposée renvoie à la section 3; la mention du chapitre pertinent (2 ?) fait défaut et doit être ajoutée.

Il pourrait par ailleurs être ajoutée la nécessité de tenir un registre des indisponibilités des plateformes.

Par ailleurs, le canton de Genève souligne ici la problématique sécuritaire qui pourrait se poser dans le cadre de la transmission des images de vidéosurveillance. En effet, l'office cantonal de la détention en particulier est régulièrement amené à transmettre des enregistrements des images de vidéosurveillance, de ses établissements pénitentiaires aux autorités pénales ou administratives. Autoriser un accès illimité de ces images aux parties via une plateforme pourrait engendrer un problème sécuritaire, dans la mesure où celles-ci auraient la possibilité d'analyser la disposition des locaux, ainsi que l'organisation des établissements et de leurs dispositifs sécuritaires. Le canton de Genève préconise donc que, lors de la mise en place du nouveau système de communication, l'accès à ces images de vidéosurveillance soit limité.

Ad article 14 **Contrôle antivirus**

Remarque générale

Du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants.

1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse ne pourrait garantir l'opération pour des raisons techniques (espace de stockage, etc.) et interromprait l'analyse. Le processus d'analyse pourrait en outre prendre tellement de temps que le respect des délais serait compromis en cas d'utilisation de la plateforme quelques minutes avant l'échéance d'un délai.

2. Analyse limitée des fichiers volumineux : un fichier dépassant la taille maximale fixée est divisé en blocs inférieurs ou égaux à la taille maximale fixée, chaque bloc pouvant ainsi faire l'objet, de manière individuelle, de l'analyse de logiciels malveillants. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisatrices et utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :

    - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
    - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analysés pour permettre la détection de logiciels malveillants, car ils sont chiffrés.
    - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
    - En raison des mesures de protection, des fichiers seront rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».

Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail classique, Dropbox...). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, avant et après leur transmission par la plateforme. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus.

Ad alinéa premier

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne doit pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra du logiciel chargé de la division et de la vérification. Cette limite évoluera de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels. Elle doit donc pouvoir être adaptée facilement.

L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets~~ à effectuent un contrôle antivirus.*

Ad alinéa 2

La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants paraît d'ores et déjà trop basse au regard des possibilités techniques actuelles. Cette limite peut et sera facilement augmentée par les exploitants de la plateforme.

L'alinéa 2 doit donc être supprimé :

> ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~

Ad alinéa 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est absolument nécessaire.

La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est en l'état pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

L'alinéa 4 devrait donc être libellé comme suit :

> [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels.

Ad alinéa 5

Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, le motif de la non-transmission devrait être précisé (voir ci-dessus les commentaires à l'art. 5 al. 2 let. d ch. 2).

Ad article 15 **Calcul de l'émolument**

Remarque générale sur le calcul des émoluments

Le calcul des émoluments se fonde sur les articles 6 et 32 de la LPCJ. Les coûts de la plateforme sont répartis entre les cantons utilisateurs. Pour les membres de la corporation, la part des émoluments est calculée sur la base de la population résidante permanente. Avec les non-membres, la corporation conclut une convention conformément à l'article 6 de la LPCJ. L'indemnisation

convenue doit couvrir l'ensemble des frais (y compris les frais d'investissement, FF 2023 679, p. 22) occasionnés par les non-membres. Les coûts pour les non-membres seront donc généralement plus élevés que ceux des membres.

Ad alinéa premier

Il y a lieu d'harmoniser les versions allemande et française de cette disposition, dont la cohérence terminologique doit en outre être garantie. Pour plus de clarté, il est proposé de scinder l'alinéa 1 en deux alinéas, le texte proposé étant le suivant :

> *[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement ~~de~~ de la plateforme centralisée ~~et~~ et permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public. ~~Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~.*
> *[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.*

Ad alinéa 3 (alinéa 2 du projet)

L'alinéa 2 du projet devient l'alinéa 3. Il est en outre proposé de le modifier comme suit :

> *[3] Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans, ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.*

Ad alinéa 4 (alinéa 3 du projet)

L'alinéa 3 du projet devient l'alinéa 4. Il est en outre proposé de le modifier comme suit :

> *[34] Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~il~~ ne couvrent pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.*

Ad article 16 Répartition de l'émolument

Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération. La part fédérale de 10% est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen.

Le canton de Genève est favorable à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, il souligne que seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixera le montant annuel des émoluments. Il tiendra compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17).

La formulation suivante est proposée :

[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :
a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;
b. tribunaux de la Confédération : 5 % ;
c. cantons : 90 %.
[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation de droit public proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû; est déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.
[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.

Ad article 19 **Échéance**

L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du code des obligations s'appliquent par analogie.

Il est donc proposé d'adopter le libellé suivant pour cette disposition :

[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.
[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.
[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.

Ad article 22 **Numérisation de documents physiques**

Cette disposition concerne toutes les autorités qui mènent des procédures dont le droit procédural est soumis à la LPCJ (art. 2 LPCJ). Pour les cantons, ce sont le code de procédure civile, la loi sur l'aide aux victimes et le code de procédure pénale qui priment.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. Les spécifications techniques de la numérisation devraient figurer dans une ordonnance départementale, étant précisé que la seule mention d'une résolution minimale ne semble pas suffisante pour garantir la qualité de la reconnaissance de texte.

Ad article 22a (nouveau) **Renvoi de documents physiques (nouveau)**

Problématique

Le chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7) indique qu'il a été renoncé à intégrer dans l'ordonnance une disposition relative à l'interprétation restrictive de l'article 30 LPCJ car il n'y aurait plus de marge de manœuvre légale à cet effet. Cette constatation

se réfère à l'interprétation de la notion de « documents » figurant à l'article 30, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents.

Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent sans nul doute une marge d'interprétation téléologique des dispositions de la LPCJ.

En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme « justitia.swiss ». Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur.

Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, la LPCJ instaurera de nouvelles obligations de renvoi, qui n'existent pas dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur.

Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine.

Même dans le cas, plutôt rare, où des divergences surgiraient a posteriori quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité.

La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ.

L'article 30, alinéa 2, LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce.

En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraînerait une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur.

Solution proposée

Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2, LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il est nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans

l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable.

Article 22a Renvoi des documents physiques

Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement, prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.

Ad article 22b (nouveau) **Notification de copies papier de documents originaux générés par voie électronique (nouveau)**

Problématique

Le chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7) précise que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k, nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (...) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, nCPC contient une disposition similaire pour les décisions des tribunaux civils.

L'article 22 concrétise l'article 29 LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme.

Toutefois, lorsque des particuliers ne souhaitent pas s'inscrire sur une plateforme de transmission électronique, ils conserveront à l'avenir le droit de se voir remettre un exemplaire papier des communications et des décisions. En particulier, les autorités pénales chargées des contraventions et les ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers parce que, selon l'interprétation (désormais abandonnée) des dispositions procédurales applicables de l'ordonnance, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers qui pourront être gérés par voie électronique. C'est notamment dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore.

Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s'agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d'interpréter l'exigence de signature de manière si restrictive qu'elle freine tout progrès, en contradiction avec la volonté du législateur.

Il ressort de l'article 22, alinéa 2, LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L'exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l'authentification à l'aide d'un moyen d'identification électronique reconnu ainsi que l'apposition d'un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023 ; FF 2023 679ss, remarques préliminaires concernant l'art. 22, p. 30). Il en résulte que le cachet électronique

réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n'y a donc plus de place pour un recours à l'article 14 CO dans le champ d'application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ).

Solution proposée

Il convient de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendues lorsqu'elles sont envoyées en original sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi.

Aujourd'hui déjà, il est d'usage auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une nouvelle obligation est créée dans le monde analogique. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique.

Cela ne peut avoir été l'intention du législateur.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), lequel reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier.

La solution proposée présente l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier.

Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b:

> ***Article 22b*** *Notification de copies papier de documents créés par voie électronique*
>
> *Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent*

obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.

Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet d'ordonnance, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.

Modification du titre du chapitre 2

Au vu des propositions qui précèdent, le titre du chapitre 2 devrait être modifié comme suit :

Chapitre 2 Numérisation et renvoi de documents physiques, envoi papier de documents créés par voie électronique

Ad articles 23 et 24

Problématique

Les autorités judiciaires ont sollicité et obtenu, pendant les travaux parlementaires portant sur la LPCJ, que certaines communications entre autorités, sur un plan intracantonal (procédure civile) ou même intercantonal (procédure pénale), puissent intervenir sous forme électronique sans recourir à une plateforme au sens de la LPCJ. La manière dont le projet d'ordonnance concrétise cette alternative autorisée est incompréhensible. Le champ d'application respectif des articles 23 et 24 du projet n'est pas défini. Les exigences posées à l'article 23 réduisent à néant l'intérêt de toute communication électronique alternative et imposent aux autorités judiciaires des conditions et modalités aussi restrictives que la plateforme, alors même que cette voie différente devrait permettre des échanges facilités entre autorités, sans impact procédural pour les parties. La formulation proposée paraît reposer sur une méconnaissance du terrain et des processus judiciaires. Son maintien aboutirait nécessairement à des problématiques pratiques difficilement surmontables et à des contentieux supplémentaires.

Le canton de Genève invite l'office fédéral de la justice à reprendre langue avec le projet Justitia 4.0 et son groupe d'experts, de manière à clarifier les besoins et les cas métier envisagés par les autorités judiciaires lorsqu'elles ont sollicité des commissions parlementaires une voie alternative à l'usage d'une plateforme pour certaines communications entre autorités. Il y aura dans tous les cas lieu de tenir compte des remarques qui suivent.

Ad article 23 Exigences

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI).

Cette disposition devrait viser la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'acte d'enquête du ministère public à la police ou lors de la transmission des rapports de police au ministère public).

Un deuxième champ d'application est la chaîne civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte

déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

La transmission physique des dossiers entre les autorités pénales s'effectue actuellement par la Poste, par courrier interne ou par porteur. Le mandat d'acte d'enquête confié à la police pour une mesure d'instruction est généralement formulé par écrit mais l'heure exacte de son expédition et de sa réception n'a pas d'importance. De la même manière, la police transmet au ministère public ses rapports sans enregistrement de l'heure et sans délivrance de quittance. Ces communications internes n'ont pas d'impact procédural et ne modifient pas les droits et obligations des parties. Les exigences posées par le projet ne se justifient aucunement.

Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faut toutefois appliquer d'autres exigences que pour la communication via la plateforme. La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, aucune quittance n'est nécessaire. L'enregistrement dans les logfiles du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 doit en outre être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.

Ad article 24 Transmission par voie électronique entre les autorités

Comme indiqué, le champ d'application de cette disposition n'est pas défini et son articulation avec l'article 23 est obscure.

L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. supra ad article 6).

Ad article 28 Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme centrale pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.

III. Fin d'accréditation des autres moyens de communication électronique dans le cadre de procédures civiles et pénales

Le canton de Genève insiste pour que la plateforme justitia.swiss soit le moyen de communication exclusif dans les procédures civiles et pénales et qu'aucune phase transitoire ne soit prévue permettant d'opter pour les moyens actuels (PrivaSphère et IncaMail).

kanton glarus

Telefon 055 646 60 11/12/15
E-Mail: staatskanzlei@gl.ch
www.gl.ch

Regierungsrat
Rathaus
8750 Glarus

Eidgenössisches Justiz- und
Polizeidepartement
3003 Bern

Glarus, 16. Juni 2026
Unsere Ref: 2026-83 / SKGEKO.5199

Vernehmlassung i. S. Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Hochgeachteter Herr Bundesrat
Sehr geehrte Damen und Herren

Das Eidgenössische Justiz- und Polizeidepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen.

Der Regierungsrat begrüsst die Schaffung einer einheitlichen Grundlage für die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren. Zum Verordnungsentwurf nimmt er wie folgt Stellung:

Vorab verweisen wir auf die Stellungnahme der Schweizerischen Staatsanwaltschaftskonferenz (SSK) vom 20. Mai 2026, welcher wir uns anschliessen. Im Weiteren machen wir auf die nachfolgenden Aspekte aufmerksam.

Art. 2 Abs. 1 Bst. c (Anforderungen an die Plattform)
Die vorgesehene Begrenzung auf Dokumente bis zwei Gigabyte ist im Moment für die meisten Verfahren ausreichend. Insbesondere in Strafverfahren kommen jedoch bereits heute digitale Beweismittel vor, deren Datenvolumen diese Grenze deutlich überschreiten. Es wäre dem Publikum kaum vermittelbar, wenn solche Beweismittel nicht über die Plattform übermittelt werden könnten, obwohl die elektronische Kommunikation und die digitale Aktenführung als zentrale Elemente der Justizdigitalisierung kommuniziert werden. Angesichts der fortschreitenden Digitalisierung ist mit einer Zunahme umfangreicher digitaler Beweismittel zu rechnen. Wir regen an, die Grössenbeschränkung zu überprüfen.

Art. 5 Abs. 2 Bst. b und Art. 9 Abs. 4 (Organisation)
Die Verwendung des Begriffs «Organisation» ist unklar. Insbesondere bei anwaltlicher Vertretung stellt sich die Frage, ob damit die vertretene Mandantschaft oder die Anwaltskanzlei gemeint ist. Rechtsanwältinnen und Rechtsanwälte handeln im Gerichtsverfahren grundsätzlich für ihre Mandantschaft und nicht für ihre Kanzlei. Zudem sind zahlreiche Kanzleien als Unkostengemeinschaften organisiert, und die Mandate werden von den einzelnen Anwältinnen und Anwälten eigenständig geführt. Der Regierungsrat empfiehlt die Bestimmungen zu präzisieren.

Art. 14 (Virenprüfung)
Da die Plattform nur für Dokumente bis 64 Megabyte zwingend eine Virenprüfung vornehmen muss, werden die Kantone eigene Prüfmechanismen vorsehen müssen. Dies führt zu vermeidbaren Doppelspurigkeiten. Es ist deshalb zwingend anzustreben, dass die Plattform eine umfassende Virenprüfung sicherstellt.

Art. 23 (Eignungsvoraussetzungen)
Die Bestimmung orientiert sich stark an der technischen Ausgestaltung der zentralen Plattform. Für die elektronische Weitergabe innerhalb eines Kantons oder zwischen Strafbehörden sollten jedoch auch andere technische Lösungen zulässig sein. Erfolgt die Weitergabe beispielsweise durch die Mutation von Zugriffsrechten auf einer gemeinsamen Datenbank, erscheint ein synchronisierter Zeitstempel unnötig. Art. 23 sollte daher klarstellen, dass solche Lösungen zulässig sind.

Art. 24 (Elektronische Übermittlung unter Behörden)
Art. 24 stellt strengere Anforderungen auf als Art. 23, ohne dass hierfür ein sachlicher Grund ersichtlich ist. Die Voraussetzungen für die elektronische Übermittlung unter Behörden sollten sich an Art. 23 orientieren und nicht darüber hinausgehen.

Genehmigen Sie, hochgeachteter Herr Bundesrat, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

Dr. Markus Heer	Arpad Baranyi
Landammann	Ratsschreiber

E-Mail an (PDF- und Word-Version): cornelia.perler@bj.admin.ch

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
9. Juni 2026	10. Juni 2026	415/2026

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
3003 Bern

Per E-Mail (PDF- und Word-Version) an:

cornelia.perler@admin.ch

Vernehmlassung EJPD - Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)
Stellungnahme

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie uns die Möglichkeit eingeräumt, zum Entwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (E-VEKJ) Stellung zu nehmen.

1. Allgemeine Anmerkungen

Die fortschreitende Digitalisierung der Justiz und der Verwaltung erfordert zeitgemässe, sichere und praktikable Rahmenbedingungen für den elektronischen Rechtsverkehr und die elektronische Aktenführung. Die vorgeschlagenen Regelungen tragen diesem Bedürfnis grundsätzlich Rechnung, indem sie eine zweckmässige Grundlage für eine effiziente elektronische Kommunikation in den Justizverfahren schaffen. Der Vernehmlassungsentwurf erscheint insgesamt sachgerecht und praktikabel und wird vom Kanton Graubünden ausdrücklich begrüsst.

2. Anmerkungen zu den einzelnen Bestimmungen

Zu den einzelnen Bestimmungen beantragen wir folgende Änderungen:

Art. 2 Anforderungen an die Plattform

Abs. 1 lit. b

Art. 2 Abs. 1 lit. b sieht vor, dass die Dokumente auf den Plattformen gemäss dem Bundesgesetz über die elektronische Kommunikation in der Justiz (BEKJ; SR 172.023) nach dem technischen Standard der Bundesverwaltung verschlüsselt werden. Aus unserer Sicht wäre eine offenere Formulierung wünschenswert, da künftig womöglich nicht nur die zentrale Plattform gemäss Art. 3 BEKJ und die Plattform nach Art. 6a des Verwaltungsverfahrensgesetzes (VwVG; SR 172.021) betrieben werden, sondern auch weitere Plattformen, die sich stärker an kantonalen Standards orientieren. Deshalb sollten die Anforderungen zumindest so formuliert werden, dass sie auch die technischen Standards der Verschlüsselung der Kantone erfassen, soweit diese den bundesrechtlichen Standards entsprechen.

Wir schlagen deshalb vor, Art. 2 Abs. 1 lit. b wie folgt zu ergänzen:

> «Die Dokumente auf der Plattform werden nach dem technischen Standard der Plattform **oder einem gleichwertigen Standard** verschlüsselt; (…)»

Abs. 1 lit. c

Im erläuternden Bericht wird zutreffend darauf hingewiesen, dass forensische Beweismittel in Strafverfahren – insbesondere Abbilder beschlagnahmter Computer oder Mobiltelefone – regelmässig die vorgesehene Grössenbeschränkung von 2 Gigabyte pro Dokument überschreiten. Der erläuternde Bericht hält weiter fest, dass Plattformbetreiberinnen und -betreiber die Übermittlung grösserer Dateien für bestimmte Benutzerinnen und Benutzer ermöglichen können (Erläuternder Bericht, S. 11).

Diese Möglichkeit ist, insbesondere für Strafverfolgungsbehörden, von erheblicher Bedeutung. Sie sollte deshalb nicht nur im erläuternden Bericht erwähnt, sondern ausdrücklich auf Verordnungsstufe vorgesehen werden.

Hierzu könnte beispielsweise folgende Regelung in Art. 2 Abs. 1 lit. c E-VEKJ aufgenommen werden:

> «Die Plattform kann **standardmässig** bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln. **Sie ermöglicht bei Bedarf und nach vorgängiger Absprache auch die Entgegennahme und Übermittlung grösserer Dokumente**.»

Abs. 1 lit. d

Die in dieser Bestimmung vorgesehene Löschfunktion ist eine Funktionalität, welche – wenn überhaupt – im 3. Abschnitt der E-VEKJ geregelt werden sollte. Zudem ist der Wortlaut der Bestimmung nach unserer Beurteilung zu absolut formuliert und kaum umsetzbar. Wie der erläuternde Bericht auf Seite 11 ausführt, wird durch die Löschfunktion nur die erteilte individuelle Berechtigung gelöscht, nicht das Dokument als solches. Zudem wäre bei der Löschung nach unserer Beurteilung zwischen den Behörden und anderen Benutzerinnen und Benutzern zu unterscheiden. Art. 2 Abs. 2 lit. d E-VEKJ sollte deshalb überprüft und angepasst, allenfalls gestrichen werden.

Abs. 2

Art. 2 Abs. 2 E-VEKJ sieht vor, dass das Eidgenössische Justiz- und Polizeidepartement (EJPD) die funktionellen und betrieblichen Anforderungen an die Plattformen, einschliesslich der Schnittstellen nach Art. 19 Abs. 1 und 2 BEKJ, regelt. Diese Bestimmung erscheint uns sachgerecht. Bei deren Umsetzung wird das EJPD zu beachten haben, dass die Kantone von den erlassenen Bestimmungen stark betroffen sein werden. Deshalb sind sie bei deren Erlass in geeigneter Form miteinzubeziehen.

Art. 3 Betriebsbewilligung, Anforderungen an die Plattformen

Im erläuternden Bericht wird festgehalten, das EJPD werde im Rahmen der Umsetzung des Bewilligungsverfahrens prüfen, ob ein Merkblatt erarbeitet werden solle, das die Bewilligungsvoraussetzungen detailliert zusammenfasse (S. 6).

Der Kanton Graubünden würde die Ausarbeitung eines solchen Merkblatts sehr begrüssen. Ein Merkblatt würde massgeblich zu einer einheitlichen und praxisnahen An-

wendung der Bewilligungsvoraussetzungen beitragen, das Bewilligungsverfahren erleichtern und die Kantone bei der Ausgestaltung geeigneter Übermittlungsformen für erstinstanzliche Verwaltungsverfahren unterstützen. Es wäre daher sowohl für die Umsetzung des BEKJ als auch die Digitalisierung der kantonalen Verwaltungsverfahren wertvoll, wenn das EJPD ein Merkblatt zu den Bewilligungsvoraussetzungen ausarbeiten würde. Der Kanton Graubünden bittet das EJPD, ein entsprechendes Merkblatt zu verfassen.

Art. 4 Format der Dokumente

Abs. 1

Die Festlegung des Formats PDF/A für Dokumente von Behörden und der Formate PDF und PDF/A für die weiteren Benutzerinnen und Benutzer wird begrüsst.

Abs. 2

Der Bundesrat schlägt vor, dass Beilagen in jeder Form eingereicht und übermittelt werden können. Diese Regelung sollte nach unserer Beurteilung überprüft werden. In vielen Fällen lässt sich der Informationsgehalt eines Dokuments im Format PDF rechtsgenüglich wiedergegeben. Die Einreichung der Beilagen in diesem verbreiteten Standardformat erleichtert die Fallbearbeitung erheblich. Den Verfahrensbeteiligten liegt dasselbe Dokument vor, Konversionen durch Behörden entfallen und die digitale Aktenführung wird vereinfacht. Dies entspricht dem Ziel der Digitalisierung, Verfahren effizienter und schneller abzuwickeln. Zudem können Geschäftsverwaltungssysteme aus Sicherheitsgründen nur mit einer beschränkten Anzahl an Dateiformaten umgehen. Eine freie Wahl der Dateiformate würde die Bearbeitung erschweren und zusätzliche IT-Sicherheitsrisiken schaffen. Deshalb sollten Beilagen – wie die von den Benutzerinnen und Benutzern erstellten Dokumente – grundsätzlich im Format PDF eingereicht werden.

Eine Ausnahme ist für Fälle vorzusehen, in denen sich der Informationsgehalt einer Beilage nicht vollständig und korrekt in einem PDF-Dokument wiedergeben lässt. Dies trifft insbesondere auf Audio- oder Videoaufnahmen, Tunnelüberwachungen und Daten aus Fahrzeugsystemen zu. Für solche Fallkonstellationen ist vorzusehen, dass Beilagen ausnahmsweise im Originalformat eingereicht werden können.

Darüber hinaus erscheint eine spezielle Regelung für strukturierte Daten erforderlich. Die Ausführungen im erläuternden Bericht deuten darauf hin, dass strukturierte Daten als Beilagen im Sinne von Art. 4 Abs. 2 E-VEKJ gelten (vgl. S. 15 f.). Trifft dies zu, sollte in Art. 4 Abs. 2 VERV ausdrücklich vorgesehen werden, dass strukturierte Daten stets in einer geeigneten maschinenlesbaren Form eingereicht und übermittelt werden können. Denn für eine effiziente Fallbearbeitung ist die elektronische Übermittlung strukturierter Daten von erheblicher praktischer Bedeutung; sie darf keinesfalls erschwert werden.

Im Weiteren muss es möglich sein, sämtliche Informationen einzureichen, welche für technische Nachweise erforderlich sind.

Aus diesen Gründen schlagen wir vor, Art. 4 folgendermassen anzupassen:

«Format der eingereichten Dokumente

[1] Die verfahrensleitenden und die verfahrensbeteiligten Behörden erstellen ihre Dokumente zur Übermittlung an die Plattformen im Format PDF/A, die übrigen Verfahrensbeteiligten im Format PDF oder PDF/A.

[2] Beweismittel sind grundsätzlich im Format PDF einzureichen. Ist dieses ungeeignet, den Inhalt korrekt wiederzugeben, können sie ausnahmsweise im Originalformat eingereicht werden.

[3] Strukturierte Daten dürfen zusätzlich in geeigneter maschinenlesbarer Form eingereicht werden. Zusätzliche technische Informationen dürfen übermittelt werden, soweit diese für technische Nachweise erforderlich sind.

Bearbeitung eingereichter Dokumente

[1] Die verfahrensleitende Behörde muss folgende Formate bearbeiten können:

a. schriftliche Unterlagen: PDF, PDF/A;
b. Bilddateien: BMP, GIF, JPEG, PNG;
c. Audiodateien: MP3, OGG, WAV;
d. Videodateien: AVI, MOV, MKV, MP4;
e. Archivdateien: ZIP, 7z.

[2] Wird eine Beilage in einem anderen Format eingereicht und kann die verfahrensleitende Behörde diese nicht zweckmässig bearbeiten, so fordert sie die einreichende Person oder Behörde auf, die Beilage in einem festgelegten Format erneut einzureichen oder den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen.

[3] Sie setzt hierfür eine angemessene Frist an.»

Art. 5 Quittungen

Abs. 2 lit. d Ziff. 2

Im erläuternden Bericht wird festgehalten, dass Dokumente mit Schadsoftware nicht übermittelt werden. Solche Dokumente würden zwar auf der Eingangsquittung aufgeführt, jedoch lediglich mit Dateinamen und Dateigrösse (S. 17).

Diese Regelung erscheint uns ergänzungsbedürftig. Auch bei Dokumenten, deren Übermittlung aufgrund des Ergebnisses der Virenprüfung verweigert wurde, sollte der Hashwert in der Quittung ausgewiesen werden. Nur so lässt sich insbesondere bei geltend gemachten Fehlfunktionen der Virenprüfung nachvollziehen, welche Datei hochgeladen wurde. Dies dient der Transparenz und der Nachvollziehbarkeit des Übermittlungsvorgangs. Nach unserer Beurteilung sollten daher in der Eingangsquittung die zugehörigen Hashwerte auch bei nicht übermittelten Dokumenten aufgenommen werden. Art. 5 Abs. 2 lit. d Ziff. 2 E-VEKJ ist entsprechend anzupassen.

Abs. 2 lit. g

Bei Vertretungsverhältnissen sollten auf der Quittung sowohl die handelnde Person als auch die vertretene Person ausgewiesen werden. Dadurch wird die Nachvollziehbarkeit des Übermittlungsvorgangs verbessert und das zugrunde liegende Vertretungsverhältnis eindeutig dokumentiert. Art. 5 Abs. 2 lit. g E-VEKJ ist entsprechend anzupassen.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Der Bundesrat geht davon aus, dass sowohl verfahrensleitende als auch verfahrensbeteiligte Behörden ihre Dokumente vor der Übermittlung über die zentrale Plattform mit einem geregelten elektronischen Siegel und einem qualifizierten elektronischen Zeitstempel nach dem Bundesgesetz über die elektronische Signatur (ZertES;

SR 943.03) zu versehen haben. Dies hätte zur Folge, dass grundsätzlich sämtliche Schweizer Behörden mit einem geregelten behördlichen Siegel ausgestattet werden müssten. Für den Kanton Graubünden wäre dies mit einem erheblichen organisatorischen und finanziellen Aufwand verbunden.

Der Bundesrat stützt diese Auffassung auf Art. 22 Absatz 2 BEKJ. Nach Sinn und Zweck dieser Bestimmung kann sich die Pflicht zur Verwendung eines geregelten elektronischen Siegels und eines qualifizierten elektronischen Zeitstempels jedoch nur auf verfahrensleitende Behörden beziehen. Das elektronische Siegel gewährleistet Herkunft, Zeitpunkt, Integrität und Authentizität eines Dokuments. Da Verfügungen und Entscheide verfahrensleitender Behörden Rechte und Pflichten begründen und über das konkrete Verfahren hinaus Wirkung entfalten, muss ihre Echtheit jederzeit überprüfbar sein. In diesen Fällen erscheint die elektronische Siegelung sachgerecht und erforderlich.

Verfahrensbeteiligte Behörden nehmen demgegenüber keine autoritative Funktion wahr. Die von ihnen eingereichten Unterlagen begründen regelmässig keine neuen Rechte oder Pflichten. In der Praxis handelt es sich meist um Registerauszüge, Akten früherer Verfahren oder bereits eröffnete Entscheide. Die Authentifizierung über die zentrale Plattform gewährleistet eine ausreichende Identifikation der absendenden Behörde. Zweifel an Echtheit oder Integrität einzelner Dokumente können – wie bei den anderen Verfahrensbeteiligten – im Rahmen der Beweiswürdigung geklärt werden, wenn sich dies als erforderlich erweist. Eine Siegelung ist in diesen Fällen nicht geboten.

Art. 22 Abs. 2 BEKJ ist daher dahingehend auszulegen, dass die Siegelungspflicht nur für verfahrensleitende Behörden gilt. Infolgedessen ist Art. 6 E-VEKJ ist folgendermassen zu ergänzen:

> Übermittelt eine **verfahrensleitende** Behörde mehrere Dokumente zusammen an eine Plattform, so reicht es, wenn nur ein Dokument über ein Siegel und einen Zeitstempel verfügt.

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Die Authentifizierung über AGOV ist sinnvoll und zielführend. Fraglich erscheint, ob dies in dieser Form in der VEKJ abzubilden ist. Aus unserer Sicht wäre es besser, allgemeine Anforderungen an die Authentifizierungsqualität vorzusehen oder einen Verweis auf das «Level of Assurance 3 nach dem eCH-0170 V2» aufzunehmen. Die konkrete technische Ausgestaltung könnte das EJPD auf Verordnungsebene festlegen.

Art. 9 Profile

Abs. 2

Diese Regelung bezieht sich nur auf verfahrensleitende Behörden, da nach unserer Auffassung nur diese Behörde die zu übermittelnden Dokumente vor der Übermittlung zu siegeln und mit einem Zeitstempel zu versehen haben (vgl. dazu die Ausführungen zu Art. 6).

Bei den verfahrensleitenden Behörden ist auf die verpflichtende Angabe einer postalischen Adresse zu verzichten. Die postalische Adresse eignet sich bei Behörden nicht als verlässliches Identifikationsmerkmal. Eine Behörde kann trotz mehrerer Standorte oder Postadressen lediglich über ein einziges Profil verfügen. Umgekehrt kann es sachgerecht sein, für dieselbe Postadresse mehrere Profile zu führen.

Eine Behörde kann ausserdem über das im Profil hinterlegte Siegel eindeutig identifiziert werden. Die zusätzliche Angabe einer postalischen Adresse ist deshalb für die Identifikation nicht erforderlich und sollte nicht vorgeschrieben werden.

Wir schlagen daher vor, Art. 9 Abs. 3 E-VEKJ folgendermassen anzupassen:

Die Profile von **verfahrensleitenden** Behörden müssen mindestens folgende Angaben enthalten:

a. Name der Behörde;

~~b. Postadresse;~~

~~c.~~b. Bezeichnung ihres Siegels.

Art. 12 Maximale Aufbewahrungsdauer für Dokumente und Quittungen

Artikel 12 E-VEKJ sieht vor, Dokumente und Quittungen sechs Monate nach der Entgegennahme bzw. Erstellung automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die BEKJ-Plattformen ein «Briefkasten» und keine Langzeitablage sein sollen.

Für Quittungen erscheint uns eine sechsmonatige Aufbewahrungsdauer indessen als unzureichend. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Natürlich müssen die verfahrensleitenden Behörden und die Verfahrensparteien darum besorgt sein, Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch vorkommen, dass Quittungen – wie etwa bei einer Zustellung – nicht heruntergeladen werden. Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von den Plattformen selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen. Deshalb würden wir es begrüssen, wenn Quittungen – entsprechend der bei der Schweizerischen Post im Briefverkehr für Nachforschungen geltenden Regelung – während drei Jahren auf den Plattformen aufbewahrt werden würden.

Art. 14 Virenprüfung

Soweit für uns ersichtlich, verpflichtet Art. 14 E-VEKJ die Plattformen lediglich dazu, Dokumente im Zeitpunkt der Übermittlung einer Virenprüfung zu unterziehen. Sollte diese Auslegung zutreffen, bietet Art. 14 E-VEKJ keinen hinreichenden Schutz vor Malware. Nach unserer Beurteilung sollten Dokumente während der gesamten Aufbewahrungsdauer periodisch auf Malware geprüft werden. Nur so kann sichergestellt werden, dass Aktualisierungen auf den Malware-Signaturen auf den gesamten Dokumentenstamm angewendet werden.

Art. 14 Abs. 3 E-VEKJ sieht zudem vor, dass die Betreiberin der Plattform auf Ersuchen der Benutzerin oder des Benutzers auf eine Virenprüfung verzichten kann. Diese Regelung ist nach unserer Beurteilung zu grösszügig. Ein solcher Verzicht sollte ausschliesslich auf Ebene einzelner Dokumente zulässig sein. Art. 14 Abs. 3 E-VEKJ ist entsprechend anzupassen.

Schliesslich erachten wir es als erforderlich, dass sämtliche ungeprüften Dateien und Dokumente auch über Schnittstellen (APIs) hinweg klar als solche gekennzeichnet werden. Gegebenenfalls sollte deren Zugriff nur über einen zweistufigen Prozess ermöglicht werden.

Art. 22 Digitalisierung von physischen Dokumenten

Art. 22 E-VEKJ konkretisiert Art. 29 BEKJ. Dieser bezieht sich ausschliesslich auf die verfahrensleitenden Behörden (vgl. BBl 2023 679/36). Dies kommt im Wortlaut von Art. 22 E-VEKJ nicht zum Ausdruck. Bei isolierter Betrachtung von Art. 22 E-VEKJ entsteht daher der Eindruck, dass die entsprechenden Anforderungen auch von den verfahrensbeteiligten Behörden und den anderen Benutzerinnen sowie Benutzern zu erfüllen sind. Um dieses Missverständnis zu vermeiden, sollte die fragliche Regelung ausdrücklich auf die verfahrensleitenden Behörden begrenzt werden.

Hierzu könnte Art. 22 Abs. 1 z.B. folgendermassen angepasst werden:

> Dieses Kapitel gilt für die Digitalisierung von physischen Dokumenten **durch die verfahrensleitenden Behörden** in Verfahren, in welchen eine Plattform nach Artikel 1 zu nutzen ist.

Art. 23/24 Verwendung von anderen Lösungen zur Übermittlung von Dokumenten

Das Verhältnis zwischen Art. 23 und Art. 24 E-VEKJ ist unklar. Die Marginalien legen nahe, dass Art. 23 E-VEKJ allgemeine Anforderungen an die Eignung alternativer elektronischer Übermittlungsformen formuliert, während Art. 24 E-VEKJ die elektronische Übermittlung unter Behörden normiert. Soweit ersichtlich trifft dies nicht zu. Art. 23 E-VEKJ scheint vielmehr die elektronische Kommunikation innerhalb der zivilrechtlichen und strafprozessualen Verfahrenskette zu regeln (vgl. Art. 128b Abs. 2 der Schweizerischen Zivilprozessordnung [ZPO; SR 272], Art. 103b Abs. 2 der Schweizerischen Strafprozessordnung [StPO; SR 312.0] sowie Art. 8c Abs. 2 des Opferhilfegesetzes [OHG; SR 312.5]), während sich Art. 24 E-VEKJ auf die übrigen Formen des elektronischen Datenaustauschs bezieht. Dies sollte sich in der Marginalie der beiden Regelungen widerspiegeln.

Im Übrigen orientiert sich Art. 23 E-VEKJ stark an der technischen Lösung der zentralen Plattform nach Art. 3 BEKJ. Für die elektronische Weitergabe innerhalb kantonaler Verfahren sollten jedoch andere Anforderungen gelten als für die Kommunikation über eine externe Plattform (z.B. Kommunikation Berufsbeistandschaft und Kindes- und Erwachsenenschutzbehörde, Kantonspolizei und Staatsanwaltshaft). Hier kann der Datenaustausch z.B. auch durch die Mutation von Zugriffsrechten auf einer gemeinsamen kantonalen Datenbank erfolgen. Bei dieser Form des Datenaustauschs sind Quittungen entbehrlich; die Protokollierung in den Logfiles des kantonalen IT-Systems genügt. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem wiederholten Versand von Dokumenten über eine externe Plattform vorzuziehen. Diese Möglichkeit des Datenaustauschs sollte weder durch Art. 23 noch Art. 24 E-VEKJ ausgeschlossen werden. Die fraglichen Regelungen sind entsprechend anzupassen.

Verworfene Regulierungsideen

Rücksendung von physischen Dokumenten

Bei der Ausarbeitung der VEKJ wurde geprüft, ob in der VEKJ eine Bestimmung aufgenommen werden kann, die es erlaubt, auf die Rücksendung physischer Dokumente zu verzichten. Die Aufnahme einer solchen Bestimmung wurde jedoch verworfen, weil Art. 30 BEKJ ein solches Vorgehen ausschliesse (S. 7).

Dieses Ergebnis ist zu bedauern. In der Praxis werden häufig nicht Originale, sondern lediglich Kopien von Schriftstücken eingereicht. Selbst wenn Originaldokumente eingereicht werden, verfügen die absendenden Personen oder Behörden in aller Regel bereits über Kopien oder anderweitige Reproduktionen. Es ist daher davon auszugehen, dass retournierte Unterlagen vielfach keinen praktischen Nutzen mehr haben und regelmässig entsorgt werden.

Hinzu kommt, dass physisch eingereichte Dokumente insbesondere im Strafverfahren heute nur ausnahmsweise zurückgesandt werden. Würde das BEKJ ohne einschränkende Auslegung verstanden, führte dies faktisch zur Einführung neuer Rücksendungspflichten im papierbasierten Verfahren, die derzeit nicht bestehen. Dass mit dem BEKJ eine solche Ausdehnung angestrebt wurde, ist nicht anzunehmen.

Aus diesen Gründen würde es der Kanton Graubünden ausserordentlich begrüssen, wenn in die VEKJ eine Regelung aufgenommen würde, welche die Rücksendung von physischen Dokumenten auf jene Fälle beschränkt, in denen sie tatsächlich erforderlich ist. Eine generelle Rücksendepflicht würde einen erheblichen Mehraufwand verursachen, ohne dass ein entsprechender praktischer Nutzen erkennbar wäre.

Versand in Papierform

Im erläuternden Bericht hält der Bundesrat fest, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen (S. 7 f.).

In der Tat verlangen die massgeblichen Verfahrensbestimmung die Unterschrift der ausstellenden Person bzw. des Gerichts, falls eine Entscheidung auf Papier versendet wird (vgl. Art. 238 lit. h ZPO, Art. 80 Abs. 2 und Art. 201 Abs. 2 lit. h StPO). Die Unterzeichnungspflicht darf die gesetzlich vorgesehene elektronische Aktenführung aber nicht ihres praktischen Nutzens entleeren, soweit die mit der Unterzeichnung verfolgten Zwecke hinreichend gewahrt bleiben. Die Unterzeichnung dient insbesondere der Authentifizierung des Entscheids, der Zurechnung zur ausstellenden Person sowie der Dokumentation der Verantwortungsübernahme. Diese Funktionen können auch durch eine qualifizierte elektronische Signatur erfüllt werden.

Der bestehende Auslegungsspielraum spricht daher dafür, den verfahrensleitenden Behörden zumindest zu gestatten, Entscheide auch beim Versand auf Papier mit einer qualifizierten elektronischen Signatur zu versehen. Dadurch kann sowohl den Anforderungen der Unterzeichnungsvorschrift als auch der gesetzlich vorgesehenen elektronischen Aktenführung Rechnung getragen werden.

Der Bundesrat wird gebeten, im erläuternden Bericht zur VEKJ klarzustellen, dass eine solche Praxis rechtskonform ist. Sollten weitergehende Erleichterungen bei den Unterzeichnungserfordernissen möglich sein, würde der Kanton Graubünden diese ausdrücklich begrüssen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und ersuchen Sie um Berücksichtigung unserer Anliegen.

Für allfällige Rückfragen steht Ihnen Christa Baumann (christa.baumann@djsg.gr.ch, Tel. 081 257 25 09) gerne zur Verfügung.

Freundliche Grüsse

Namens der Regierung

Der Präsident:	Der Kanzleidirektor:
Martin Bühler	Daniel Spadin

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont

t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Hôtel du Gouvernement – Rue de l'Hôpital 2, 2800 Delémont

Département fédéral de justice et police DFJP
Monsieur le Conseiller fédéral
Beat Jans
Palais fédéral ouest
3003 Berne

par courriel à cornelia.perler@bj.admin.ch

Delémont, le 16 juin 2026

Consultation – Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,
Mesdames, Messieurs,

Par la présente, le Gouvernement de la République et Canton du Jura vous transmet sa réponse relative à la procédure de consultation citée en marge.

Le Gouvernement relève qu'il adhère, dans une large mesure, aux remarques et propositions formulées dans le document d'aide aux autorités cantonales à la prise de position dans le cadre de la consultation élaboré par l'équipe de projet Justitia 4.0, auquel il peut être renvoyé pour le surplus.

Cela étant, certaines dispositions appellent des commentaires particuliers qui sont exposés ci-dessous.

Article 4

La question du contrôle des formats transmis par la plateforme « justitia.swiss » mérite d'être précisée, notamment s'agissant de l'exigence du format PDF/A pour le document principal de la transaction.

En l'état, une incertitude subsiste quant au risque de refus d'un dépôt pour des motifs purement techniques liés au format du fichier transmis. Cette problématique apparaît particulièrement sensible pour les documents cachetés ou certaines pièces numériques dont le contenu ou la structure ne permettent pas toujours une conversion adéquate en PDF/A.

Par ailleurs, la transmission de fichiers dans des formats éditables (p. ex. Word ou Excel) soulève des enjeux de sécurité, notamment en présence de macros ou de contenus actifs. Des précisions complémentaires concernant les mécanismes de contrôle, de validation et de sécurisation prévus par la plateforme seraient bienvenues.

Article 5

Le champ d'application exact de la notion de « plateforme » gagnerait à être clarifié, notamment afin de déterminer si les échanges automatisés ou internes entre applications judiciaires sont également soumis aux exigences prévues par l'OCEP en matière de quittances, de sécurité et de traçabilité.

Les interactions entre les articles 5, 23 et 24 mériteraient également d'être précisées afin d'éviter toute incertitude d'interprétation. Les nombreuses exigences techniques et organisationnelles liées aux plateformes (conservation des preuves de transmission et de consultation, ouverture des délais, etc.) soulèvent en effet des questions importantes quant à leur mise en œuvre concrète et à leur impact opérationnel pour les autorités judiciaires.

Article 22

Concernant les documents créés électroniquement puis transmis sous forme papier, une clarification explicite serait bienvenue afin de confirmer que le cachet électronique réglementé, au sens de la LPCJ, remplace les exigences de signature individuelle, indépendamment du support utilisé.

Article 23

La portée exacte de cette disposition mériterait d'être clarifiée, notamment s'agissant des solutions techniques admissibles pour les échanges électroniques entre autorités judiciaires.

En particulier, la notion selon laquelle la transmission peut être « attestée d'une autre manière » figurant à la lettre a gagnerait à être précisée. Il conviendrait notamment de clarifier si une journalisation technique ou des traces applicatives peuvent être considérées comme suffisantes au regard des exigences de l'OCEP.

Article 24

Les exceptions prévues à l'article 103c, alinéa 2, CPP mériteraient d'être davantage précisées, en particulier pour les autorités communales disposant d'un pouvoir répressif.

En effet, les discussions préparatoires évoquaient la possibilité pour le Conseil fédéral de prévoir des exceptions ou des modalités particulières pour certaines autorités. À ce stade, les contours de ces dérogations ne paraissent toutefois pas clairement définis.

Article 26

Les exigences prévues à l'article 26 apparaissent particulièrement détaillées et pourraient entraîner des impacts organisationnels et financiers importants pour les cantons. Leur mise en œuvre pourrait notamment nécessiter le déploiement de solutions spécifiques de signature ou d'attestation électronique dans de nombreux contextes opérationnels, tels que les audiences, auditions ou perquisitions.

Ces exigences soulèvent d'importants enjeux techniques, organisationnels et financiers, qui nécessiteront une préparation et une planification suffisantes de la part des autorités concernées.

Remarque sur la forme

Au surplus, le Gouvernement se permet de signaler le détail de forme suivant :

- Article 7, alinéa 1 : il conviendrait d'ajuster la terminologie utilisée, dans la mesure où la notion de « document séparé » semble en réalité renvoyer à une quittance de réception ou de consultation émise par la plateforme.

Pour terminer, le Gouvernement est favorable à une entrée en vigueur de l'ordonnance au 1er juillet 2027, en cohérence avec l'entrée en vigueur prévue de la LPCJ. Ce délai apparaît nécessaire afin de permettre aux cantons et aux autorités concernées de finaliser les adaptations organisationnelles et techniques requises et d'assurer une mise en conformité adéquate des processus et outils concernés.

Tout en vous remerciant de prendre note de ce qui précède, le Gouvernement vous remercie de l'avoir consulté et vous prie de croire, Monsieur le Conseiller fédéral, Mesdames, Messieurs, à l'expression de sa haute considération.

AU NOM DU GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

Rosalie Beuret Siess
Présidente

Jean-Baptiste Maître
Chancelier d'État

Annexe : document d'aide aux autorités cantonales à la prise de position dans le cadre de la consultation élaboré par l'équipe de projet Justitia 4.0

Plateforme de communication électronique dans le domaine judiciaire : consultation sur l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Document d'aide aux autorités cantonales à la prise de position dans le cadre de la consultation

Lors de sa séance du 13 mars 2026, le Conseil fédéral a ouvert la consultation sur l'avant-projet de l'OCEP (AP-OCEP). Les prises de position peuvent être déposées jusqu'au 22 juin 2026.

Le présent d'aide a pour but d'aider les autorités cantonales et les autres milieux intéressés lors de l'élaboration leur prise de position. Il contient pour l'essentiel des explications et des suggestions concernant les différents articles de l'ordonnance ainsi que des propositions de formulation, mais ne constitue pas la prise de position du projet Justitia 4.0.

Auteurs

Autorités cantonales: Alexandra Altherr Müller, Tribunal des assurances sociales/ZH, Patrick Becker, Secrétariat général du Pouvoir judiciaire genevois/GE, Jan Grunder, Tribunal régional Oberland/BE, Stéphane Nakamura, Tribunal de l'arrondissement de la Gruyère/FR, Marc Tille, Service juridique de la sécurité et de la justice/VS, Serge Segura, Tribunal cantonal/VD, Daniel Stehlin, Ministère public/BL, Stephan Walder, Ministère public/ZH, André Zumthurm, Tribunal cantonal/LU

Equipe de projet Justitia 4.0: Jérôme Barraud, Chantal Neuschwander, Christian Renggli, Houri Rousseau

Commentaires, suggestions et propositions de formulation

Préambule

Le projet d'ordonnance omet délibérément de citer les articles qui confèrent au Conseil fédéral la compétence de réglementer le format des documents transmis par voie électronique. Le rapport explicatif précise que, « *pour conserver une vue d'ensemble* », le préambule ne mentionne que les dispositions des lois de procédure qui traitent de la communication en dehors des plateformes de la LPCJ. Même si une référence générale à la LPCJ semble appropriée, il serait préférable de mentionner toutes les normes de délégation contenues dans les lois de procédure. Cela vaut en particulier pour les articles qui confèrent au Conseil fédéral la compétence de définir les formats ; ceux-ci devraient donc logiquement être également mentionnés dans le préambule.

Le préambule devrait dès lors être libellé comme suit:

> *vu la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ),*
>
> *vu l'art. 6a, al. 2, 21a, al. 2 et 34, al. 1bis de la loi du 20 décembre 1968 sur la procédure administrative du 20 décembre 1968 (PA),*
>
> *vu l'art. 38e de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF),*
>
> *vu les art. 128b, al. 3, et 128c, al. 2 et 128e du code de procédure civile du 19 décembre 2008 (CPC),*
>
> *vu les art. 33a, al. 4, 33b, 33c, al. 2 et 34, al. 3, de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),*
>
> *vu les art. 76a, al. 2, 103b, al. 3, et 103c, al. 2 et 103e du code de procédure pénale du 5 octobre 2007 (CPP),*
>
> *vu l'art. 2e de la loi fédérale du 23 décembre 2011 sur la protection extraprocédurale des témoins (Ltém),*

vu l'art. 31f de la loi fédérale du 22 mars 1974 sur le droit pénal administratif,
vu les art. 8c, al. 3, et 8d, al. 2, et 8f de la loi du 23 mars 2007 sur l'aide aux victimes (LAVI),
vu les art. 37d et 38a, al. 2, de la procédure pénale militaire du 23 mars 1979 (PPM),

Chapitre 1 Exploitation et utilisation de plateformes

Section 1 Champ d'application

Art. 1

Selon notre interprétation, l'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral et **ne s'applique donc pas aux cantons**. La valeur ajoutée de l'alinéa 3 n'est pas évidente, étant donné qu'en cas de divergence une loi prévaudrait de toute façon sur la présente ordonnance.

Section 2 Autorisation d'exploiter

Art. 2 Conditions applicables aux plateformes

Les conditions applicables aux plateformes semblent appropriées. Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre c, devrait être fixée dans une annexe à la présente ordonnance ou dans une ordonnance du DFJP.

La fonction de suppression visée à l'alinéa 1, lettre d, est une fonctionnalité qui, le cas échéant, devrait être réglementée dans la section 3 de la présente ordonnance. Par ailleurs, la formulation de cette disposition est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport à la page 11, la fonction de suppression efface l'autorisation individuelle accordée, mais pas le document en tant que tel. Il conviendrait également, s'agissant de la suppression, de faire la distinction entre les autorités et les autres utilisateurs.

Art. 3 Procédure d'autorisation

Pas de remarque.

Section 3 Documents, quittances et apposition d'un cachet

Art. 4 Format des documents

Le présent projet utilise – à l'instar de la LPCJ – le terme « document » plutôt que « fichier » (cf. message LPCJ, p. 20), en invoquant que le terme « fichier » est un terme trop technique pour être utilisé dans la loi.

Le terme « fichier » est préférable dans l'ordonnance, dans la mesure où il s'agit d'aspects techniques des pièces transmises.

Al. 1

Nous sommes favorables à la définition du format PDF/A pour les documents des autorités et des formats PDF et PDF/A pour les autres participants à la procédure.

Al. 2

Dans de nombreux cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Dans ces cas, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. Si les parties soumettent leurs pièces jointes

au format PDF, la conversion par les autorités judiciaires n'est plus nécessaire et toutes les parties disposent du même document. La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si en règle générale les documents sont disponibles au format PDF, cela permet un traitement rapide par les avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers. Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. De plus, le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées.

Dans certains cas particuliers, le format PDF ne permet pas de restituer suffisamment le contenu informatif d'un document. On peut penser par exemple à des enregistrements audio ou vidéo, à des vidéosurveillances multipistes de tunnels ou à des enregistrements provenant de voitures électriques. Dans ces cas, le DFJP devrait définir quels formats de fichiers peuvent être transmis directement via la plateforme. Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format Zip.

Les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centrale.

L'alinéa 2 devrait donc être libellé comme suit :

> [2] ~~*Les annexes peuvent être remises dans n'importe quel format*~~ *Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine*.

Al. 3 et 4

La sélection proposée de formats de fichiers est adéquate, mais le niveau de norme retenu est critiquable. La définition des formats que les autorités chargées de la procédure doivent traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP.

La liste des formats de documents pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.). Il est nettement plus facile de gérer cela dans une annexe que dans le corps de la présente ordonnance.

Les alinéas 3 et 4 devraient donc être libellés comme suit :

> [3] ~~*L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :*~~*Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour qu'elle puisse la transmettre dans un format défini par l'autorité.*
>
> ~~*a. documents écrits : PDF, PDF/A ;*~~
>
> ~~*b. images : BMP, GIF, JPEG, PNG ;*~~
>
> ~~*c. fichiers audio : MP3, OGG, WAV ;*~~
>
> ~~*d. fichiers vidéo : AVI, MOV, MKV, MP4 ;*~~

~~*c. fichiers d'archives : ZIP, 7z.*~~

[4] ~~*Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée*~~ *Le DFJP définit les formats de fichiers à transmettre via la plateforme.*

[5] ~~*L'autorité qui dirige la procédure fixe un délai approprié.*~~

Art. 5 Quittances

Nous sommes favorables à la réglementation proposée. Il est important que **le nom de la personne responsable d'une autorité**, au sens de l'alinéa 2, lettre b, **ne figure pas** dans la quittance. Seul le nom de l'autorité devrait apparaître sur la quittance.

Un résultat positif lors du contrôle antivirus visé à l'alinéa 2, lettre d, chiffre 2, constitue un motif possible de rejet par la plateforme, mais pas le seul. La taille ou le format du fichier peuvent également en être la cause.

L'alinéa 2, lettre d, chiffre 2 précise que les documents qui n'ont pas été transmis sont mentionnés dans la quittance de réception. Cette disposition comporte une erreur logique. Les documents non transmis ne peuvent pas figurer sur la **quittance de réception**, puisqu'ils n'ont justement **pas été transmis**. Par conséquent, la quittance ne peut contenir la valeur de hachage de fichiers qui n'ont pas été transmis. Si la plateforme ne parvient pas à transmettre un ou plusieurs documents, l'expéditeur reçoit un message de la plateforme, mais pas de quittance. Le chiffre 2 doit donc être supprimé.

[2] *Les quittances comportent en particulier les données suivantes:*

a. *le type de quittance ;*

b. *le nom de l'expéditeur, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit;*

c. *le nom du destinataire ou de son entreprise et son adresse sur la plateforme;*

d. *pour la quittance de réception :*

1. *la liste des documents transmis, leur taille et leur valeur de hachage,*

~~*2. laliste des documents qui n'ont pas été transmis en raison du résultat du contrôle antivirus, avec indication de leur taille,*~~

~~*3.*~~*2. le moment de la transmission à la plateforme;*

e. *…*

f. *…*

g. *…*

Les plateformes doivent à l'avenir pouvoir également transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car les fichiers XML, pour des raisons techniques, ne peuvent pas être cachetés.

Art. 6 Apposition d'un cachet par l'autorité expéditrice

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur

l'un des documents transmis **avant** leur envoi à la plateforme; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement. La plateforme au contraire appose un cachet **après** la transmission à via la plateforme, sur la quittance émise sur la base de l'article 5.

L'article 6 règle **l'apposition d'un cachet sur les documents** par l'autorité dirigeant la procédure **avant leur transmission via une plateforme** (art. 22 al.2 LPCJ). Le projet mentionne que lors que plusieurs documents sont transmis, il suffit qu'un des de ces documents soit muni d'un cachet, ce qui est est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examiné indépendamment de la plateforme.

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Par ailleurs l'obligation d'apposer un cachet imposée aux autorités qui dirigent la procédure ainsi qu'aux autorités qui y participent est en contradiction avec le concept technique de la plateforme centralisée.

Pour diverses fonctionnalités de la plateforme centralisée, **la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure** est essentielle. Ainsi, seules les autorités qui dirigent la procédure peuvent procéder à des notifications. Seules les adresse des autorités qui dirigent la procédure sont visibles pour les tiers dans le répertoire public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités participant à la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations et particuliers et indépendamment d'une procédure (judicaire). Cela ouvrirait la plateforme à toute communication électronique entre autorités, pour laquelle la LPCJ n'offre toutefois pas de base légale suffisante. L'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires.

Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents. L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision incidente ou le jugement d'une autorité qui dirige la procédure crée des droits et des obligations. Ceux-ci produisent leurs effets au-delà de la procédure en cause. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète ou de la plateforme centralisée, si le document en question est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités agissent de manière autoritaire.

Les autorités participant à la procédure ne peuvent en revanche pas être tenues d'apposer un cachet électronique sur leurs documents. Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent généralement pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante.

Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante pour équiper l'ensemble des autorités suisses d'un cachet électronique. L'instauration généralisée d'un cachet électronique entraînerait pour les cantons un effort organisationnel considérable et des coûts importants.

Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond pas au concept de la LPCJ, laquelle ne prescrit aucune fonctionnalité permettant à la plateforme de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre via la plateforme.

Il serait cependant utile de préciser comment les autorités peuvent signer des documents qui, selon la jurisprudence actuelle, doivent porter la signature de leur auteur, comme les expertises (BSK StPO-Heer, art. 187 N 1). Dans le cas des instituts de médecine légale ou de l'Institut fédéral de métrologie METAS, par exemple, ces expertises peuvent tout à fait être réalisées par des autorités ou, à tout le moins, par des « services administratifs ». Dans ces cas, l'identité de l'expert qui établit l'expertise est déterminante, raison pour laquelle la signature électronique qualifiée (contrairement au commentaire de l'art. 22 LPCJ dans le message, FF 2023 679ss, p. 30) devrait probablement continuer à s'appliquer à l'avenir.

Il est important de souligner la différence entre l'envoi et consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents lors de la consultation en ligne du dossier.

Art. 7 Apposition d'un cachet par la plateforme

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement (art. 6). La plateforme, en revanche, appose son cachet **après** la transmission sur la plateforme, sur la quittance de réception émise, qui est régie par l'article 5.

Al. 1

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la **quittance, jamais le document transmis.** Dans le cas de la plateforme centralisée, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

Al. 2

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. **L'alinéa. 2 doit donc être supprimé**.

> ~~[2] *Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.*~~

Section 4 Authentification, profils, interfaces et attribution de droits

Art. 8 Authentification des utilisateurs

L'authentification via AGOV conformément à l'aliné 1 est, de notre point de vue, jugée judicieuse et pertinente.

L'utilisation éventuelle de services d'authentification supplémentaires dans le cadre de futures plateformes cantonales, conformément à l'alinéa 2, est saluée.

À l'avenir, la plupart des autorités seront reliées à la plateforme via une interface. La disposition proposée à l'alinéa 3 laisse une marge de manœuvre suffisante pour mettre en œuvre de futures solutions techniques.

Art. 9 Profils

Al. 2

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, car une autorité peut disposer de plusieurs sites. La disposition doit être adaptée en conséquence:

[2] Les profils des autorités comprennent au moins les données suivantes :

a. le nom de l'autorité ;

~~b. l'adresse postale ;~~

b ~~c~~. le nom du cachet.

Al. 3, let. a

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et administratif. Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs doit être considéré comme critique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques.

[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :

a. pour les personnes physiques : le prénom, le nom, la date de naissance ~~et l'adresse postale~~ ;

Al. 3, let. b

Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique**. Il convient donc de renoncer à l'adresse postale également pour les organisations.**

L'alinéa devrait donc être formulé comme suit:

[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :

a. pour les personnes physiques : le prénom, le nom, <u>et</u> la date de naissance ~~et l'adresse postale~~ ; …
b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Al. 4

Le sens de cet alinéa n'est pas compréhensible. Il n'est pas clair s'il s'agit du profil d'une organisation ou d'un particulier. Une clarification par le législateur semble indiquée. Le rapport mentionne la personne

responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.

Art. 10 Interface

Cet article permet aux utilisateurs de la plateforme de connecter leurs systèmes à celle-ci via une interface et d'octroyer des droits de représentation à leurs collaborateurs. Cela se fait par l'intermédiaire d'un utilisateur technique qui reçoit un mot de passe numérique (token). La réglementation proposée est donc saluée.

Art. 11 ~~Attribution~~ Confirmation et retrait de droits

La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait de parler de « confirmation » plutôt que d'« attribution ». Nous sommes favorables à la variante proposée à l'alinéa 2.

Section 5 Protection des données, sécurité des données et contrôle antivirus

Art. 12 Durée maximale de conservation des documents et des quittances

Problématique

L'article 12 du projet d'ordonnance OCEP prévoit que les documents et les quittances soient automatiquement supprimées de la plateforme à l'expiration d'un délai de six mois. Nous sommes favorables à la suppression automatique des documents après un délai raisonnable, car la plateforme est conçue comme une « boîte aux lettres » et non comme un moyen d'archivage à long terme. Il semble cependant opportun, en ce qui concerne les quittances, de prévoir un délai plus long. Les quittances peuvent encore être nécessaires très tard dans la procédure, par exemple pour prouver le respect d'un délai ou la prise de connaissance d'un document donné. Bien entendu, les autorités doivent veiller à transférer les quittances dans leurs propres logiciels de gestion d'affaires. Cependant, le fait que, en raison du fonctionnement de la plateforme centralisée, elles ne soient pas classées dans les dossiers d'une procédure, par exemple en cas de notifications, peut conduire à ce que le téléchargement des quittances ne soit pas effectué. Contrairement aux requêtes et aux notifications, qui peuvent être renvoyées depuis les systèmes sources, les quittances générées par la plateforme elle-même seraient dans ce cas déjà perdues au bout de six mois. A ce stade-là, une procédure n'est souvent pas encore terminée.

Les quittances peuvent également contenir des données personnelles (telles que les noms des parties à la procédure), ce qui, dans le contexte des procédures judiciaires, peut même en faire des données personnelles particulièrement sensibles. Cependant, ces données, tout comme les pièces du dossier elles-mêmes, bien plus sensibles, sont stockées de manière sécurisée sur la plateforme. À cela s'ajoute le fait que les quittances constituent également de très petites quantités de données qui ne nécessitent pas de stockage supplémentaire important, même si elles restent disponibles longtemps sur la plateforme.

Solution proposée

Il est proposé ici de modifier ou de compléter l'article 12 AP-OCEP en s'alignant sur délai de suppression de trois pendant lequel la Poste suisse permet d'effectuer des recherches dans le courrier. En français le fait que la suppression est automatique manque dans le libellé de l'alinéa 1 et devrait être complété comme suit:

> *Art. 12 Durée maximale de conservation des documents et des quittances*
>
> *[1] Les documents ~~et les quittances~~ enregistrés sur une plateforme sont automatiquement ~~détruits~~supprimés six mois après leur réception ~~ou leur délivrance~~.*

[2] Lorsque des documents peuvent être consultés, l'autorité qui dirige la procédure fixe le délai pendant lequel ils sont disponibles sur la plateforme. Passé ce délai, ils sont automatiquement supprimés ~~détruits~~.

[3] Les quittances sont automatiquement supprimées trois ans après leur délivrance.

Al. 2

Nous sommes favorable à solution proposée. Il n'est pas nécessaire de prévoir une prolongation du délai dans l'ordonnance, car l'autorité peut ordonner une deuxième consultation du dossier avec les mêmes pièces.

Art. 13 Sécurité des données

La disposition proposée renvoie à la section 3; la mention du chapitre pertinent (2 ?) fait défaut et devrait être ajoutée.

Art. 14 Contrôle antivirus

Du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants.

1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse atteindrait sa limite (espace de stockage, etc.), interromprait l'analyse et le processus d'analyse pourrait prendre tellement de temps que le respect des délais serait compromis en cas de soumission dans l'urgence.

2. Analyse limitée des fichiers volumineux : un fichier qui dépasse la taille maximale fixée est divisé en blocs gérables aux fins de l'analyse de logiciels malveillants, lesquels sont ensuite analysés individuellement. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisatrices et utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :

    - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
    - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analyser pour détecter de logiciels malveillants, car ils sont chiffrés.
    - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
    - En raison des mesures de protection, des fichiers sont rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».

Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail

classique, Dropbox…). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et **cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, respectivement avant et après leur transmission via la plateforme**. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus.

Al. 1

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne devrait pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra fortement du logiciel chargé de la division et de la vérification. Cette limite évoluera également de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels, et devrait pouvoir être facilement adaptée.

L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets à~~ effectuent un contrôle antivirus.*

Al. 2

La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants peut (et devrait) être facilement augmentée par les exploitants de la plateforme en fonction des possibilités techniques et de l'expérience opérationnelle croissante. **L'alinéa 2 doit donc être supprimé**.

> ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~

Al. 3

Pas de remarque.

Al. 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est essentielle selon nous. La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

L'alinéa 4 devrait donc être libellé comme suit :

> [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels.

Al. 5

Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, il ne s'agit manifestement pas d'une quittance, puisqu'aucun document n'a été transmis (voir les commentaires aux art. 5, al. 2, let. d, ch. 2, ci-dessus).

Section 6 Émolument pour l'utilisation de la plateforme centralisée

Le calcul des émoluments se fonde sur les articles 6 et 32 de la LPCJ. Les coûts de la plateforme sont répartis entre les cantons utilisateurs. Pour les membres de la corporation, la part des émoluments est calculée sur la base de la population résidante permanente. Avec les non-membres, la corporation conclut une convention conformément à l'article 6 de la LPCJ. L'indemnisation convenue doit couvrir l'ensemble des frais (y compris les frais d'investissement, FF 2023 679, p. 22) occasionnés par les non-membres. Les coûts pour les non-membres seront donc généralement plus élevés que ceux des membres.

Art. 15 Calcul de l'émolument

Les versions allemande et française ont été comparées et harmonisées ; cela vaut également pour la cohérence terminologique des notions y figurant. Pour plus de clarté, l'alinéa 1 a été scindé en deux (nouveaux) alinéas.

La référence à la planification financière triennale pour la fixation du montant total de l'émolument pour trois ans est saluée. Cette approche fournit une base prévisible et réaliste pour l'émolument fixé annuellement selon la clé de répartition figurant à l'article 16. Au surplus, la mesure corrective prévue à l'alinéa 4 garantit une capacité d'adapter l'émolument si nécessaire.

Le texte suivant est proposé :

> *[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement ~~-~~ de la plateforme centralisée ~~-~~ et permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public~~. Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~.*
>
> *[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.*
>
> *[3]Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.*
>
> *[3~~4~~] Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~il~~ ne couvrent pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.*

Art. 16 Répartition de l'émolument

Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération, mais pas pour les procédures administratives de première instance. La part fédérale de 10 % est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen.

Nous sommes favorables à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixe le montant annuel des émoluments; il tient compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-

membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17).

La formulation suivante est proposée :

> *[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :*
>
> *a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;*
>
> *b. tribunaux de la Confédération : 5 % ;*
>
> *c. cantons : 90 %.*
>
> *[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation public proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû ; est déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.*
>
> *[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.*

Art. 17 Part de l'administration fédérale et du MPC

Aucune remarque.

Art. 18 Part des tribunaux de la Confédération

Aucune remarque.

Art. 19 Échéance

L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du code des obligations s'appliquent par analogie. Il est donc proposé d'adopter le libellé suivant pour cette disposition :

> *[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.*
>
> *[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.*
>
> *[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.*

Art. 20 Service comptable cantonal

Aucune remarque.

Art. 21 Évaluation des règles de calcul de l'émolument

Nous sommes favorables à la révision du mode de calcul de l'émolument proposée.

Chapitre 2 Numérisation et renvoi de documents physiques, envoi papier de documents créés par voie électronique

Art. 22 Numérisation de documents physiques

Cette disposition concerne toutes les autorités qui mènent des procédures dont le droit procédural est déclaré applicable par la LPCJ (art. 2 LPCJ). Pour les cantons, ce sont donc le Code de procédure civile, la Loi sur l'aide aux victimes et le Code de procédure pénale qui priment.

Le format PDF/A prescrit à l'alinéa 2 facilite l'archivage des dossiers judiciaires. Il n'est toutefois pas certain que ce format puisse être facilement traité par les applications judiciaires cantonales, qui sont très différentes les unes des autres.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. La résolution de 300 dpi semble judicieuse. Il convient de noter qu'avec une résolution de 300 dpi, la taille du fichier est quatre fois supérieure à celle obtenue avec une résolution de 150 dpi.

Art. 22*a* Renvoi de documents physiques (nouveau)

Problématique

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est indiqué qu'il a été renoncé à intégrer dans l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (AP-OECP) une disposition relative à l'interprétation restrictive de l'article 30 LPCJ, car il n'y avait plus de marge de manœuvre légale à cet effet.

Cette constatation se réfère à l'interprétation de la notion de « documents » contenue dans l'article 30 de la LPCJ, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents. Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas encore dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent tout à fait une marge d'interprétation des dispositions de la LPCJ dans le sens de leur objectif législatif.

En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme «justitia.swiss». Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur.

Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, une loi visant à introduire les communications judiciaires électroniques instaurera de nouvelles obligations de renvoi dans le processus papier, qui n'existaient pas encore dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur.

Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc très majoritairement jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine.

Même dans le cas, plutôt rare, où des divergences surgiraient a posteriori quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents

renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité.

La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ.

L'article 30, alInéa 2, de la LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce.

En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraîne une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur.

Solution proposée

Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2, de la LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il semble nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable.

> […]***Art. 22a*** *Renvoi des documents physiques*
>
> *Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.*

Art. 22*b* – Notification de copies papier de documents originaux générés par voie électronique (nouveau)

Problématique :

Comment joindre les personnes qui ne sont pas joignables sur la plateforme ?

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est précisé que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k du nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (…) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, du nCPC contient une disposition similaire pour les décisions des tribunaux civils.

L'article 22 concrétise l'article 29 de la LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme. Toutefois, lorsque des particuliers ne souhaitent pas

s’inscrire sur une plateforme de transmission électronique, ils conserveront à l’avenir le droit de se voir remettre un exemplaire papier des communications et des décisions.

En particulier, les autorités pénales chargées des contraventions et les services des ordonnances pénales des ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers, parce que, selon l’interprétation (désormais abandonnée) des dispositions procédurales applicables par l’ordonnance relative à la LPCJ, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers pouvant être gérés par voie électronique. C’est notamment dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore.

Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s’agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d’interpréter l’exigence de signature de manière si restrictive qu’elle freine tout progrès.

Il ressort de l'article 22, alinéa 2, LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L’exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l’authentification à l’aide d’un moyen d’identification électronique reconnu ainsi que l’apposition d’un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023 ; FF 2023 679ss, remarques préliminaires concernant l’art. 22, p. 30). Il en résulte que le cachet électronique réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n’y a donc plus de place pour un recours à l’article 14 CO dans le champ d’application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ).

Solution proposée

Il convient certes de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendures lorsqu'elles sont envoyées **sous forme d'original** sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi.

Aujourd'hui déjà, il est d'usage courant auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une **nouvelle obligation est créée dans le monde analogique**. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique. Cela ne peut avoir été l'intention du législateur.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), qui reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier.

La solution proposée présenterait l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier.

Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b:

> ***Art. 22b*** *Notification de copies papier de documents créés par voie électronique*
>
> *Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.*

Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet de l'OCEP, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.

Chapitre 3 Transmission de documents par un autre moyen qu'une plateforme au sens de la LPCJ

Section 1 Recours à d'autres solutions pour la transmission de documents

Art. 23 Exigences

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI). Nous partons du principe que cette disposition vise la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'enquête du ministère public à la police judiciaire ou lors de la transmission des résultats d'actes d'enquête que la police transmet au ministère public.

Un deuxième champ d'application est la chaîne de procédure civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

La transmission physique des dossiers entre les autorités pénales s'effectue actuellement encore souvent par la poste, par courrier interne ou par coursier. La mission confiée à la police pour une mesure d'instruction est généralement formulée par écrit, mais ni la date exacte ni la réception ne sont consignées séparément.

Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faudrait toutefois appliquer d'autres exigences que pour la communication via la plateforme.

La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, nous estimons qu'aucune quittance n'est nécessaire. L'enregistrement dans les logfiles du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 devrait être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.

Art. 24 Transmission par voie électronique entre les autorités

L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils, ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. la consultation relative à l'art. 6 OECP). Une incertitude subsiste à cet égard, notamment en ce qui concerne les corporations de droit public qui n'agissent pas dans l'exercice de la puissance publique.

Cette disposition précise les exceptions prévues à l'article 128c, alinéa 2, CPC, à l'article 103c, alinéa 2, CPP et à l'article 8d, alinéa 2, de la LAVI. Ces exceptions sont justifiées lorsque, dans le cadre de procédures civiles ou pénales, un grand nombre de communications avec les autorités sont nécessaires, communications qui ne font pas partie de la chaîne de procédure pénale ou civile, et lorsque la communication directe, par exemple via une interface, est préférable aux communications électroniques dans le domaine judiciaire via la plateforme, notamment pour la transmission de métadonnées ou pour des raisons de coût. Dans le cadre de la procédure pénale, on peut penser par exemple aux autorités fiscales ou de migration, ou encore aux grandes entreprises de transport ou aux instituts de médecine légale, qui devraient également relever de la notion d'autorité. Il en va de même pour certaines autorités fédérales telles que l'OFDF.

Les conditions devraient s'inspirer de l'article 23 et ne pas aller au-delà. En tout état de cause, on ne voit pas pourquoi l'article 24 prévoit des exigences plus strictes, étant donné que l'article 103c, alinéa 2, CPP – contrairement à l'art. 103b, alinéa 2, CPP, qui prévoit l'enregistrement du moment de transmission et la protection du dossier contre toute modification et toute consultation non autorisée – n'impose aucune exigence quant à la documentation d'une transmission.

Section 2 Transmission de documents par voie électronique dans le domaine de la poursuite pour dettes et la faillite

Art. 25

Aucune remarque.

Section 3 Attestation par voie électronique de l'exactitude du procès-verbal en procédure pénale et en procédure pénale militaire

Art. 26 Aucune remarque.

Chapitre 4 Dispositions finales

Art. 27 Abrogation et modification d'autres actes

Aucune remarque.

Art. 28 Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.

Abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures administratives

Aucune remarque.

Abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite

En raison de l'abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite, IncaMail et PrivaSphere ne pourront plus être utilisés dans les procédures engagées après l'entrée en vigueur de l'ordonnance. Il appartient donc aux cantons de choisir et de mettre à disposition des canaux appropriés pour les procédures administratives qui ne peuvent pas être traitées via la plateforme justitia.swiss.

Art. 14a Signatures et cachets électroniques vérifiés par le validateur

Aucune remarque.

Art. 14b Apposition et validation de signatures et de cachets électroniques

Aucune remarque.

KANTON
LUZERN

Justiz- und Sicherheitsdepartement
Bahnhofstrasse 15
Postfach 3768
6002 Luzern
Telefon 041 228 59 17
jsdds@lu.ch
www.lu.ch

Eidgenössisches Justiz- und Polizeidepartement

per E-Mail:
cornelia.perler@bj.admin.ch

Luzern, 16. Juni 2026

Protokoll-Nr.: 788

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrte Damen und Herren

Im Namen und Auftrag des Regierungsrates danke ich Ihnen für die Gelegenheit zur Stellungnahme und teile Ihnen zu obgenanntem Verordnungsentwurf Folgendes mit:

Wir begrüssen grundsätzlich die Konkretisierungen des Bundesgesetzes vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) durch das Verordnungsrecht.

Der Verordnungsentwurf enthält eine Vielzahl an technischen Bestimmungen. Technische Spezifikationen können jedoch einer hohen Entwicklungsdynamik unterliegen. Wir regen daher an, die angemessene Normstufe zu überprüfen. Detailvorgaben können in einem Anhang oder in der geplanten Departementsverordnung des EJPD geregelt werden. Dies gilt für technische Vorgaben wie zur Maximalgrösse übermittelter Dateien (Art. 2), zu den Dateiformaten (Art. 4), zur Siegelung durch die Plattform (Art. 7), zur Authentifizierung (Art. 8), zur Virenprüfung durch die Plattform (Art. 14) u.a.m. Dabei sollte auch geprüft werden, ob die Vorgaben vereinfacht werden können (z. B. hinsichtlich Dateiformate). Wir verweisen dafür auch auf die Liste mit weiteren Änderungshinweisen im Anhang dieses Schreibens.

Die Verordnung stellt in verschiedenen Bereichen zu strenge technische Anforderungen auf. Zu erwähnen sind insbesondere die Regelungen über die elektronische Übermittlung zwischen Behörden ausserhalb der BEKJ-Plattform. Artikel 23 VEKJ-Entwurf verlangt Quittierung und Zeitstempel. Die im Kanton Luzern in der Verwaltung eingesetzten Geschäftsverwaltungssysteme gewährleisten, dass Zeitpunkt und Umfang der Weitergabe nachvollziehbar bleiben und die Akten vor Veränderung sowie unberechtigter Kenntnisnahme geschützt sind. Diese Anforderungen sind nach unseren Erfahrungen ausreichend. Auf weitergehende Anforderungen ist zu verzichten.

Festzustellen ist ausserdem, dass die Verordnung verschiedentlich den Handlungsspielraum des Gesetzes nicht vollständig ausschöpft. Zu erwähnen sind insbesondere folgende Aspekte, die von der Verordnung differenzierter geregelt werden sollten:

- Art. 22 Abs. 2 BEKJ: Die vom Gesetz verlangte elektronische Siegelung von Dokumenten durch die Behörden sollte durch Verordnung nur für die verfahrensleitenden Behörden vorgesehen werden. Wenn generell alle Behörden ihre Dokumente vor der Übermittlung mit einem geregelten elektronischen Siegel samt qualifiziertem elektronischen Zeitstempel versehen müssen, müssten im Kanton Luzern beispielsweise sämtliche Gemeindeverwaltungen diese technischen Mitteln beschaffen, damit sie Akten über die Plattform dem Kantonsgericht zukommen lassen können. Von einer solch breiten Ausstattung war bisher noch nie die Rede. Sie wäre mit organisatorischem Aufwand und Kosten verbunden. Bei der Kategorie der übrigen Benützer bringt die Plattform Siegel und Zeitstempel selber bei der Eingabe an (Art. 22 Abs. 4 BEKJ). Zudem könnte in Zusammenhang mit dem Siegelungserfordernis geprüft werden, dass nach dem Grundsatz, wonach bei Einreichung einer Vielzahl an Dokumenten nur ein einziges gesiegelt werden muss (Art. 6 VEKJ-Entwurf) analog auch bei der Zustellung von elektronischen und physischen Entscheiden im gleichen Verfahren eine Siegelung ausreicht und sich das physische Dokument auf eine Kopie des elektronischen beschränkt. Mit dieser Vereinfachung könnte das Problem der doppelten Originale gelöst werden.
- Art. 29 und 30 BEKJ: Die im Gesetz genannte Rücksendung physisch eingereichter Dokumente nach dem elektronischen Einlesen sollte durch Verordnung differenziert werden. Eine generelle Pflicht, solche Unterlagen zurückzusenden, würde insbesondere in Strafverfahren neue Papierprozesse schaffen, die bisher in dieser Form nicht bestanden. Sie hätte keinen erkennbaren Mehrwert, würde aber erheblichen administrativen Aufwand, Portokosten und Medienbrüche verursachen. Dies widerspräche dem Ziel der Digitalisierung. Der erläuternde Bericht geht davon aus, dass im Verordnungsrecht kein Spielraum besteht, was nicht überzeugt.

Die Bestimmungen zu den Gebühren (Art. 15ff.) nehmen wir zur Kenntnis. Die Festlegung des Gesamtbetrags der jährlichen Gebühr für jeweils drei Jahre im Voraus auf der Grundlage der Finanzplanung der öffentlichen-rechtlichen Körperschaft der Plattform nach dem BEKJ und die Anpassung nur bei geändertem Bedarf erachten wir als eine praktikable Lösung.

Freundliche Grüsse



Ylfete Fanaj
Regierungsrätin

Weitere Änderungshinweise

Ingress	Der **Ingress** ist unvollständig und die Gründe dafür im erläuternden Bericht nicht nachvollziehbar erläutert. Der Ingress sollte daher mit allen Delegationsnormen ergänzt werden, insbesondere beispielweise Art. 38e nBGG (Fassung gemäss BEKJ-Änderung).
Art. 2 Anforderungen an die Plattformen	Absatz 1 lit. c: Die **Mindestanforderung von 2 GB** ist aus Sicht der Strafverfolgungsbehörden kritisch. Dateigrössen von über zwei GB entsprechen heute keineswegs mehr einem Ausnahmefall. Insbesondere Videoeinvernahmen, Auswertungen von Mobiltelefonen, Datenträgeranalysen sowie digitale forensische Sicherstellungen gehören im Bereich der Verbrechens- und Vergehenskriminalität mittlerweile zum Standard. Solche Datenmengen müssen regelmässig zwischen Polizei, Staatsanwaltschaften, Gerichten und berufsmässigen Rechtsvertreterinnen und Rechtsvertretern ausgetauscht werden. Dagegen erweist sich die Aufteilung grosser Dateien in kleinere Einheiten in der Praxis häufig als aufwendig und teilweise kaum praktikabel. Dies gilt insbesondere in zeitkritischen Verfahren wie Haftfällen oder dringlichen Zwangsmassnahmen. Die Plattformen müssen deshalb auch die unkomplizierte, jederzeitige Übermittlung sehr grosser Dateien ermöglichen und zwar ohne jegliche Bewilligungsauflagen (vgl. S. 11 erläuternder Bericht). Zudem besteht zwischen dem erläuternden Bericht und dem Verordnungstext ein gewisser Widerspruch: Während der Bericht von einer «Grössenbeschränkung» spricht, bezeichnet der Verordnungstext die Fähigkeit zur Übermittlung von zwei GB grossen Dokumenten als Mindestanforderung an die Plattform. Der Verordnungswortlaut lässt offen, ob damit eine Mindestanforderung oder zugleich eine regulatorische Obergrenze verbunden sein soll.
	Abs. 2 lit. d: Die Anforderung der **Löschung von Dokumenten und Quittungen im Profil** ist systematisch nicht sachgerecht eingeordnet. Inhaltlich betrifft sie weniger technische Anforderungen an die Plattform als vielmehr Fragen der Zugriffsberechtigungen und des Datenmanagements. Zudem ist die Bestimmung zu absolut formuliert. Wie im erläuternden Bericht zutreffend ausgeführt wird, kann regelmässig lediglich die individuelle Zugriffsberechtigung gelöscht werden, nicht jedoch das Dokument als solches. Zudem ist zwischen Behörden und übrigen Nutzerinnen und Nutzern zu unterscheiden.

Art. 4 Format der Dokumente	Abs. 2 Die **freie Formatwahl für Beilagen** erscheint zu weitgehend. Zwar können gewisse Beilagen nicht sinnvoll in ein PDF-Dateiformat überführt werden (z. B. Audio- und Videoaufnahmen, forensische Rohdaten, mehrspurige Überwachungsaufzeichnungen). Gerade in Strafverfahren können solche Daten für die Beweisführung oder die Vollzugsdokumentation wesentlich sein. In vielen Fällen kann der Informationsgehalt einer Beilage jedoch rechtsgenüglich im Format PDF wiedergegeben werden (z.B. Bilder, einfache Tabellen, Korrespondenz, Berichte, Ausdrucke elektronisch erstellter Dokumente oder Fotokopien). Werden solche Beilagen im PDF-Format eingereicht, erleichtert dies die Fallbearbeitung erheblich. Eine uneingeschränkte freie Formatwahl birgt demgegenüber erhebliche praktische und sicherheitstechnische Risiken. Geschäftsverwaltungssysteme von Gerichten, Staatsanwaltschaften und Vollzugsbehörden können aus Gründen der IT-Sicherheit regelmässig nur mit einer beschränkten Anzahl zugelassener Dateitypen umgehen. Würden Beilagen beliebig in jedem Format eingereicht, müssten die Behörden unter Umständen zunächst geeignete Programme beschaffen Es wird daher vorgeschlagen, PDF als Regelformat für Beilagen vorzusehen. Eine Übermittlung im Originalformat soll möglich bleiben, wenn PDF ungeeignet ist oder Primärdaten erforderlich sind. Abs. 2 sollte wie folgt lauten: «Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben oder sind Primärdaten erforderlich, kann die Beilage im Originalformat übermittelt werden.»
	Abs. 3: Die Formate ZIP und 7z sind nicht per se archivtaugliche Dateiformate, sondern Containerformate, in denen sich Daten platzsparend speichern und übermitteln lassen. Bei der Extraktion der komprimierten Daten aus den ZIP und 7z-Containern werden allerdings die ursprünglichen, unter Umständen nicht archivtauglichen, Dateiformate wiederhergestellt. Anstelle des Begriffs «Archivdateien» sollte in lit. e der Begriff «Containerdateien» verwendet werden.
Art. 5 Quittungen	Abs. 2 lit. d Ziff. 2: Können Dokumente aufgrund eines positiven Resultats der Virenprüfung oder aus anderen Gründen nicht übermittelt werden, fehlt es gerade an einer erfolgreichen Übermittlung, welche **Gegenstand einer Quittung** sein könnte. Die Regelung enthält insoweit einen gewissen technischen und systematischen Widerspruch. Sachgerechter erscheint deshalb eine Fehlermeldung oder Mitteilung der Plattform an die Absenderin oder den Absender, wonach einzelne Dokumente nicht verarbeitet oder nicht vollständig übermittelt werden konnten. Die Bestimmung ist zu streichen.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde	Der Grundsatz, dass bei mehreren Dokumenten die **Siegelung** eines einzigen genügt, wird als Konkretisierung von Art. 22 Abs. 2 BEKJ begrüsst. Der Wortlaut des BEKJ wie auch die Aussage im erläuternden Bericht, wonach sämtliche Dokumente aller Behörden zu siegeln seien, ist kritisch zu beurteilen, weil sie dem Konzept der zentralen Plattform widerspricht. Die Pflicht zur Siegelung sollte auf verfahrensleitende Behörden beschränkt werden. Demgegenüber erscheint eine generelle Siegelungspflicht für alle verfahrensbeteiligten Behörden (z. B. Gemeindebehörden als Vorinstanzen) nicht erforderlich. Die von ihnen in Verfahren übermittelten Dokumente begründen regelmässig keine neuen Rechte oder Pflichten, sondern bestehen typischerweise aus Registerauszügen, Akten früherer Verfahren oder (in Verwaltungsverfahren) bereits eröffneten Entscheiden. Die Authentifizierung über die Plattform genügt grundsätzlich zur Identifikation der absendenden Behörde. Somit erscheint Art. 6 zu breit beziehungsweise zu unpräzis formuliert. Klärungsbedürftig bleibt der Umgang mit Dokumenten, welche nach geltendem Recht eine persönliche Unterzeichnung der Autorenschaft voraussetzen, insbesondere Sachverständigengutachten. Schliesslich ist zwischen Versand von behördlichen Dokumenten und Akteneinsicht zu unterscheiden. Im Bereich der Akteneinsicht besteht keine Pflicht zur zusätzlichen Siegelung der Dokumente durch die verfahrensleitende Behörde. Diese Differenzierung sollte in der Verordnung oder wenigstens im erläuternden Bericht Erwähnung finden.
Art. 9 Profile	Es sollte geprüft werden, ob auf die **Angabe von Postadressen** im Behördenprofil aus Gründen der Praktikabilität verzichtet werden kann (Abs. 2 lit b). Die Postadresse bietet für die elektronische Kommunikation über die Plattform keinen wesentlichen Mehrwert. Dies gilt sinngemäss auch für die Adressen von Privatpersonen und Organisationen (Abs. 3), insbesondere im Hinblick darauf, dass bei Personen mit Wohnsitz im Ausland keine verlässliche Prüfung möglich ist.
Art. 12 Maximale Aufbewahrungsfrist	Die **automatische Löschung** von Dokumenten nach einer überschaubaren Frist ist aus Gründen des Datenschutzes, der Datensicherheit und der Begrenzung des Speicherbedarfs richtig und vom Grundsatz her, dass die Plattform kein Geschäftsverwaltungs- oder Archivsystem ist, sachgerecht. Anders zu beurteilen ist jedoch die Aufbewahrung von Quittungen. Quittungen erfüllen eine zentrale Nachweisfunktion. Gerade in Straf- und Gerichtsverfahren können solche Fragen erst deutlich später, etwa in einem Rechtsmittelverfahren oder bei der Prüfung von Fristen, relevant werden. Zu diesem Zeitpunkt ist das Verfahren häufig noch nicht abgeschlossen. Während Eingaben oder Zustellungen aus den Quellsystemen grundsätzlich erneut nachvollzogen oder reproduziert werden können, werden Quittungen von der Plattform selbst generiert. Sind sie nach sechs Monaten irreversibel gelöscht, steht die primäre Nachweisquelle nicht mehr zur Verfügung. Aus Datenschutzsicht ist zwar zu berücksichtigen, dass Quittungen Personendaten enthalten können. Gleichzeitig handelt es sich im Vergleich zu den übermittelten Aktenstücken um geringe Datenmengen, die auf der Plattform verschlüsselt gespeichert werden. Der zusätzliche Speicherbedarf einer längeren Aufbewahrung von Quittungen erscheint daher vertretbar. Es wird vorgeschlagen, die Aufbewahrungsfrist für Quittungen auf drei Jahre zu verlängern.

Art. 23 Eignungsvoraussetzungen (für Übermittlung ausserhalb einer Plattform nach dem BEKJ)	Die vorgeschlagenen Anforderungen orientieren sich stark an der technischen Logik der zentralen Plattform. Für die elektronische Weitergabe von Akten innerhalb eines Kantons und insbesondere zwischen Strafbehörden erscheinen jedoch teilweise andere Anforderungen sachgerecht. Der elektronische Austausch innerhalb bestehender kantonaler **Fachapplikationen** darf nicht unnötig erschwert werden. Insbesondere muss weiterhin möglich sein, Dokumente durch die Mutation von Zugriffsrechten auf einer gemeinsamen kantonalen Datenbank elektronisch weiterzugeben. In solchen Fällen findet kein klassischer Versand über eine Plattform statt. Weder eine separate Quittung noch der synchronisierte Zeitstempel sind erforderlich. Ausreichend ist, dass die Weitergabe beziehungsweise die Mutation der Zugriffsrechte in den Logfiles des kantonalen IT-Systems protokolliert wird. Entscheidend ist, dass Zeitpunkt und Umfang der Weitergabe nachvollziehbar bleiben und die Akten vor Veränderung sowie unberechtigter Kenntnisnahme geschützt sind. Es wird vorgeschlagen, Art. 23 zumindest dahingehend zu ergänzen, dass die elektronische Weitergabe von Dokumenten auch durch die Mutation von Zugriffsrechten auf einer gemeinsamen Datenbank zulässig ist.
Art. 24 Elektronische Übermittlung unter Behörden	Weil der **Begriff der Behörde** nicht präzisiert wird, sind Abgrenzungsfragen zu befürchten, namentlich hinsichtlich der Institutionen, die regelmässig mit Straf- oder Zivilbehörden kommunizieren, ohne klassische Verwaltungsbehörden zu sein (insbes. rechtsmedizinische Institute, psychiatrische Kliniken, öffentlich-rechtliche Transportunternehmen oder andere öffentlich-rechtlich organisierte Einrichtungen) Der persönliche Geltungsbereich der Regelung sollte daher ausdrücklich konkretisiert werden. Weiter erscheint das Verhältnis zwischen Art. 103b und Art. 103c nStPO sowie Art. 24 VE-VEKJ nicht vollständig geklärt. Während Art. 103c nStPO den Austausch von Dokumenten mit der Strafbehörde regelt, sieht Art. 24 VE-VEKJ allgemeine Sonderregelungen für den elektronischen Rechtsverkehr zwischen Behörden vor. Soweit gemäss Erläuterungsbericht auch die Kommunikation mit Gerichten ausserhalb der Plattform möglich sein soll, entstehen Abgrenzungsfragen zum klaren Wortlaut von Art. 103c nStPO sowie zur Sonderregelung von Art. 103b nStPO. Diese Punkte sollten im Verordnungstext präzisiert werden. Zudem erscheint auch der **Begriff der Person** in Art. 103d nStPO auslegungsbedürftig. Während der Titel der Bestimmung von der elektronischen Kommunikation auf Verlangen der Partei spricht, verwendet der Gesetzestext selbst den Begriff «Person». Es sollte klargestellt werden, ob darunter auch juristische Personen des Privatrechts fallen, die regelmässig mit Strafbehörden kommunizieren, ohne selbst Parteistellung im Verfahren zu haben, beispielsweise im Zusammenhang mit Editionsaufforderungen.

LE CONSEIL D'ÉTAT
DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Département fédéral de justice et police DFJP
Palais fédéral Ouest
3003 Berne

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le conseiller fédéral,

Votre correspondance du 13 mars 2026 nous est bien parvenue et nous vous remercions de nous avoir associés à la consultation susmentionnée.

Nous vous faisons part de nos remarques ci-après.

Article 2 - Conditions applicables aux plateformes

Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre *c*, devrait être fixée dans une ordonnance du DFJP.

La formulation de l'alinéa 1, lettre *d*, est trop absolue et difficilement applicable. Il conviendrait notamment de faire la distinction entre les autorités dirigeant la procédure et les autres utilisateurs.

Article 4 - Format des documents

Le terme « fichier » est préférable dans l'ordonnance, dans la mesure où il s'agit d'aspects techniques des pièces transmises.

Alinéa 1

Le ministère public relève qu'il y aurait lieu, selon lui, de prévoir la possibilité de déposer en format Excel des documents. Si les tableaux figés peuvent en effet être convertis en PDF, il existe, notamment dans des dossiers économiques, la nécessité d'intégrer au dossier des fichiers dynamiques qui ne peuvent, par essence, être figés dans un PDF.

Alinéa 2

Dans la mesure du possible, les pièces devraient être déposées également en format PDF et PDF/A, afin de faciliter le travail de toutes les parties concernées. Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des

NE

dossiers ; toutes les parties à la procédure devraient en effet d'abord rechercher le programme approprié pour ouvrir un fichier. Par ailleurs, le choix illimité des formats constituerait un risque pour la sécurité informatique de toutes les parties.

Toutefois, dans certains cas, le fichier PDF n'est pas suffisant. Dans ces cas, le DFJP devrait définir, dans une ordonnance ad hoc, après consultation de l'exploitant de la plateforme, quels formats de fichiers pourraient être transmis directement via cette dernière.

L'alinéa 2 devrait donc être libellé comme suit :

[2]*Si le format PDF ne permet pas de restituer correctement le contenu d'un document ou si les données primaires sont requises, l'annexe peut être transmise dans son format d'origine.*

Alinéas 3 et 4

La définition des formats que les autorités chargées de la procédure doivent traiter devrait figurer dans une ordonnance du DFJP.

La liste des formats de documents pris en charge sera en constante évolution. D'autres éléments techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent également être réglementés.

Article 5 - Quittances

Nous sommes favorables à la réglementation proposée. Il est important que le nom de la personne responsable d'une autorité, au sens de l'alinéa 2, lettre *b*, ne figure pas dans la quittance. Seul le nom de l'autorité devrait y apparaître.

Alinéa 2

Il est important de rappeler que les documents non transmis ne pourront, de fait, pas figurer sur la quittance de réception, puisqu'ils n'ont pas été transmis. Le chiffre 2 de la lettre *d* de cet alinéa devrait donc être supprimé.

Article 6 - Apposition d'un cachet par l'autorité expéditrice

Cet article règle l'apposition d'un cachet sur un des documents transmis par l'autorité qui dirige la procédure, découlant de l'article 22, alinéa 2 LPCJ qui doit être interprété de manière restrictive. Ceci doit donc être précisé dans l'article.

L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Il convient donc de corriger les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, dans la mesure où cela contredit le libellé de l'ordonnance, qui doit être privilégié.

Il est important de souligner la différence entre l'envoi et la consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents lors de la consultation en ligne du dossier.

Article 9 - Profils

Alinéa 2

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, car une autorité peut être sur plusieurs sites et donc disposer de plusieurs adresses. La disposition doit être adaptée en conséquence :

[2]*Les profils des autorités comprennent au moins les données suivantes :*

a. le nom de l'autorité ;
~~b. l'adresse postale ;~~
b c. le nom du cachet.

Alinéa 3, lettre *a*

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et administratif. Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur ou de l'utilisatrice. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs et d'utilisatrices doit être considéré comme critique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques.

[3]*Les profils des autres utilisateurs comprennent au moins les données suivantes :*

a. *pour les personnes physiques : le prénom, le nom et, la date de naissance ~~et l'adresse postale~~ ;*

Alinéa 3, lettre *b*

Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique. Il convient donc de renoncer à l'adresse postale également pour les organisations.

L'alinéa devrait donc être formulé comme suit :

[3]*Les profils des autres utilisateurs comprennent au moins les données suivantes :*

a. *pour les personnes physiques : le prénom, le nom, et la date de naissance ~~et l'adresse postale~~ ;*
b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Alinéa 4

Le sens de cet alinéa n'est pas compréhensible. Il n'est en effet pas clair s'il s'agit du profil d'une organisation ou d'un particulier. Une clarification par le législateur semble indiquée. Le rapport mentionne la personne responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.

Article 12 - Durée maximale de conservation des documents et des quittances

Il est proposé d'augmenter la durée de conservation des quittances au-delà de 6 mois. Il va de soi que les autorités doivent veiller à intégrer les reçus dans leur propre système et à les verser dans les dossiers. Toutefois, en cas d'omission dans l'archivage ou de besoin de données provenant de la source primaire, un délai de conservation plus long semble indiqué et il est proposé de prévoir une conservation de ces quittances pendant trois ans, ce qui correspondrait au délai prévu par la Poste pour les demandes de recherche.

Article 14 - Contrôle Antivirus

Alinéa 1

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne devrait pas être communiquée publiquement, d'une part, pour des raisons évidentes de sécurité, d'autre part, compte tenu des évolutions techniques à prévoir.

Alinéa 2

À supprimer.

Alinéa 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est essentielle selon nous. La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs et utilisatrices n'est pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

Alinéa 5

Voir commentaires ad article 5, alinéa 2.

Article 16 - Répartition de l'émolument

Les autorités judiciaires neuchâteloises sont favorables à la répartition de l'émolument entre la Confédération et les cantons, avec la possibilité de révision offerte par l'article 21, ainsi qu'avec le calcul par canton selon la population résidente permanente.

Article 21 – Évaluation

Il serait souhaitable que les cantons soient associés à l'évaluation qui sera faite par le DFJP.

Problématique du renvoi des documents physiques

D'avis des autorités judiciaires, il est essentiel de faire en sorte que l'autorité n'ait pas à renvoyer systématiquement aux parties tous les documents reçus physiquement, sous peine de les exposer à de lourdes difficultés organisationnelles. Le renvoi de documents n'a en effet aucune utilité si la finalité de ces derniers se limite à la transmission du message qu'ils contiennent. Les expéditeur-trice-s de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires à renvoyer seraient donc très majoritairement jetés dès qu'ils seraient revenus chez leurs expéditeur-trice-s d'origine.

Or, le projet d'ordonnance soumis est considéré comme lacunaire sur ce point. En effet, si l'obligation visée dans la LPCJ (art. 30, al. 1) n'est pas interprétée de manière restrictive, elle pourrait viser à instaurer en réalité de nouvelles obligations de renvoi dans le cadre de la procédure papier, obligations qui n'existent pourtant pas actuellement (en particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels). Cela ne peut pas avoir été la volonté du législateur.

Il est donc impératif, dans l'ordonnance, d'une part, de définir la notion de documents visée à l'article 30, alinéa 1 LPCJ, d'autre part, de ne prévoir le renvoi des documents déposés au format papier qu'à la condition que le déposant en ait fait expressément la demande lors du dépôt ou s'il s'agit de documents originaux officiels (documents d'identité, livrets de famille, diplômes, etc.).

Problématique de la notification de copies papier de documents créés par voie électronique

On rappellera que le concept de base de la LPCJ veut que la création électronique de dossiers doit être la norme. Cela étant, la loi a également prévu que, lorsque des particuliers ne souhaiteront pas s'inscrire sur une plateforme de transmission électronique, ils conserveront le droit de se voir remettre un exemplaire papier des communications et des décisions.

Se pose par conséquent la problématique relative à la notification, au format papier, de décisions valablement émises de façon électronique. Cette problématique est notamment vraie pour le traitement des ordonnances pénales de masse, pour qui pourtant, les effets positifs permis par un traitement numérique seraient les bienvenus.

En conséquence, il conviendra de préciser, par la création d'un nouvel article dans l'ordonnance, que la notification de documents nécessitant une signature, faite à des personnes non-enregistrées sur la plateforme, pourra continuer à se faire, au moyen d'une copie papier de l'original (qui aura été établi par voie électronique), qui restera dans le dossier numérique. Si le ou la destinataire devait avoir des doutes quant à l'authenticité de la décision, il ou elle pourrait à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permettra, en outre, de vérifier la date de création de l'original indiquée sur la copie papier.

Dans ces conditions, le ministère public propose un nouvel article qui, en substance, permettrait la possibilité de notifier des copies papier de documents originaux créés par voie électronique aux personnes avec lesquelles l'autorité ne communique pas par voie électronique. Cette notification fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent obtenir gratuitement l'original électronique via une plateforme, conformément à la LPCJ, ou demander à l'autorité un double signé à la main.

Article 23 - Exigences

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes (LAVI) et vise vraisemblablement la communication entre les autorités de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent, par exemple, être transmis à l'instance supérieure en cas de recours, ou encore lorsque d'autres autorités sont chargées de certains actes de procédure.

Le deuxième champ d'application est la chaîne de procédure civile, par exemple, lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte déterminé ou encore lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

Il convient de rappeler que la transmission électronique au sein d'un canton pourra, par exemple, s'effectuer à l'avenir par la modification des droits d'accès à l'application métier commune au sein de l'organisation (ex : Juris). Pour ce genre d'échanges, il est considéré qu'aucune quittance ne devrait être nécessaire. Le seul enregistrement dans les logfiles du système informatique cantonal suffira. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 devrait donc être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre *b*. Il convient donc de renoncer à ce critère.

Article 24 - Transmission par voie électronique entre les autorités

L'intitulé de cet article est trop général et donc trompeur. La notion d'autorité devrait par ailleurs être précisée. Cet article, tout comme cela a été dit pour l'article 23, ne devrait, dans tous les cas, pas poser des exigences que les codes de procédures et lois eux-mêmes ne prévoient pas.

Cette disposition précise les exceptions prévues à l'article 128c, alinéa 2, CPC, à l'article 103c, alinéa 2, CPP et à l'article 8d, alinéa 2, de la LAVI. Ces exceptions sont justifiées lorsque, dans le cadre de procédures civiles ou pénales, un grand nombre de communications avec les autorités sont nécessaires, communications qui ne font pas partie de la chaîne de procédure pénale ou civile, et lorsque la communication directe, par exemple via une interface, est préférable aux communications électroniques dans le domaine judiciaire via la plateforme, notamment pour la transmission de métadonnées ou pour des raisons de coût. Dans le cadre de la procédure pénale, on peut penser, par exemple, aux autorités fiscales ou de migration, ou encore aux grandes entreprises de transport ou aux instituts de médecine légale, qui devraient également relever de la notion d'autorité. Il en va de même pour certaines autorités fédérales telles que l'OFDF.

Les conditions devraient donc s'inspirer de l'article 23 et ne pas aller au-delà. En tout état de cause, on ne voit pas pourquoi l'article 24 prévoit des exigences plus strictes, étant donné que l'article 103c, alinéa 2, CPP – contrairement à l'article 103b, alinéa 2, CPP, qui prévoit l'enregistrement du moment de transmission et la protection du dossier contre toute modification et toute consultation non autorisée – n'impose aucune exigence quant à la documentation d'une transmission.

Article 28 - Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.

Tout en vous réitérant nos remerciements pour nous avoir consultés, nous vous prions de croire, Monsieur le conseiller fédéral, à l'assurance de notre parfaite considération.

Neuchâtel, le 24 juin 2026

Au nom du Conseil d'État :

Le président,
F. MAIRY

La chancelière,
S. DESPLAND

RÉPUBLIQUE ET CANTON DE NEUCHÂTEL
CONSEIL D'ÉTAT

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 16. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ). Stellungnahme

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 13. März 2026 hat das Eidgenössische Justiz- und Polizeidepartement die Kantonsregierungen eingeladen, zum Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren Stellung zu nehmen. Der Regierungsrat des Kantons Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme.

Der Regierungsrat unterstützt die Vorlage im Grundsatz. Die Umsetzung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) ist ein wichtiger Schritt hin zu durchgängig digitalen, medienbruchfreien und effizienten Justiz- und Verwaltungsverfahren. Die elektronische Kommunikation über Plattformen nach BEKJ, insbesondere über die zentrale Plattform justitia.swiss, ist für professionelle Rechtsanwenderinnen und Rechtsanwender sachgerecht und notwendig.

Aus Sicht des Regierungsrates besteht jedoch Anpassungsbedarf, damit die Verordnung in der kantonalen Praxis effizient, sicher und mit vertretbarem Aufwand umgesetzt werden kann. Dabei stehen insbesondere folgende Punkte im Vordergrund.

1 Flexible Regelung technischer Vorgaben

Technische Detailvorgaben wie Dateiformate, maximale Dateigrössen, Schnittstellen und Vorgaben zur Virenprüfung sollten nicht zu starr im Verordnungstext geregelt werden (vgl. Art. 4 Abs. 3 und 4 E-VEKJ). Sie unterliegen einem raschen technischen Wandel und müssen aufgrund der Betriebserfahrung einfach angepasst werden können. Der Regierungsrat erachtet es daher als zweckmässig, solche Einzelheiten soweit möglich in einem Anhang oder in einer Departementsverordnung des EJPD festzulegen.

2 Praxistaugliche Ausgestaltung der behördlichen Abläufe

Die Vorgaben zur Siegelung (Art. 6 und 7 E-VEKJ), zur Aufbewahrung von Quittungen (Art. 5 E-VEKJ), zur Virenprüfung (Art. 14 E-VEKJ) sowie zum Umgang mit physisch eingereichten Dokumenten (2. Kapitel E-VEKJ) sind so auszugestalten, dass sie den tatsächlichen Abläufen

der kantonalen Behörden, Gerichte und Strafverfolgungsbehörden entsprechen. Insbesondere sollen Quittungen genügend lange verfügbar bleiben, kritische oder grosse Dateien sachgerecht übermittelt werden können und die Siegelungspflicht nicht weiter reichen, als dies für die Rechtssicherheit erforderlich ist.

3 Vermeidung unnötiger Zusatzaufwände im Papierprozess

Die Einführung des elektronischen Rechtsverkehrs darf nicht dazu führen, dass für kantonale Behörden neue administrative Pflichten im Papierprozess entstehen, die weder sachlich notwendig noch mit einem erkennbaren Nutzen verbunden sind. Dies betrifft namentlich die Rücksendung physisch eingereichter Unterlagen sowie die Zustellung von Papierkopien elektronisch erzeugter Originaldokumente an Personen, die nicht elektronisch mit Behörden verkehren. Gerade in Massengeschäften ist eine praktikable Lösung erforderlich, damit das Rationalisierungspotenzial der Digitalisierung nicht wieder aufgehoben wird.

4 Fazit

Der Regierungsrat ersucht den Bund, die Anliegen der kantonalen Praxis bei der weiteren Ausarbeitung der Verordnung angemessen zu berücksichtigen. Die Verordnung soll die Digitalisierung der Justiz- und Verwaltungsverfahren wirksam unterstützen, ohne die Kantone durch unnötig starre technische Vorgaben oder unverhältnismässige organisatorische Anforderungen zu belasten.

Der Regierungsrat des Kantons Nidwalden unterstützt die Vorlage somit im Grundsatz, beantragt jedoch, sie in den erwähnten Punkten praxistauglicher, flexibler und für die Kantone mit vertretbarem Aufwand umsetzbar auszugestalten.

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme und deren Berücksichtigung.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Dr. Othmar Filliger
Landammann

lic. iur. Armin Eberli
Landschreiber

Geht an:
- cornelia.perler@bj.admin.ch

Kanton
Obwalden

Der Vorsteher des Sicherheits- und Sozialdepartements SSD

CH6060 Sarnen, Enetriederstrasse 1, SSD

Eidgenössisches Justiz- und
Polizeidepartement EJPD

Per Mail:
cornelia.perler@bj.admin.ch

Referenz/Aktenzeichen: OWSTK.5823
Unser Zeichen: ks

Sarnen, 19. Juni 2026

**Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ);
Stellungnahme.**

Sehr geehrter Herr Bundesrat

Für die Einladung zur Stellungnahme zur Änderung der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) danken wir Ihnen.

Der Kanton Obwalden befürwortet den vorliegenden Entwurf der VEKJ im Grundsatz. Zu den einzelnen Artikeln haben wir folgende Anpassungsanträge:

Ingress
Im Vorentwurf fehlen bewusst die Artikel, die dem Bundesrat die Kompetenz zur Regelung des Formats der elektronisch übermittelten Dokumente übertragen. Im erläuternden Bericht wird präzisiert, dass, "um die Übersichtlichkeit zu bewahren", im Ingress lediglich die Bestimmungen der Verfahrensgesetze erwähnt werden, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben. Auch wenn ein allgemeiner Verweis auf das BEKJ angemessen erscheint, wäre es vorzuziehen, alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen. Dies gilt insbesondere für die Artikel, die dem Bundesrat die Kompetenz zur Festlegung der Formate übertragen; diese sollten daher ebenfalls im Ingress erwähnt werden.

Art. 4 Format der Dokumente
Der Vorentwurf verwendet – wie das BEKJ – den Begriff "Dokument" anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: "Der Begriff "Datei" ist für das

Sicherheits- und Sozialdepartement SSD
Enetriederstrasse 1, 6060 Sarnen
Tel. +41 41 666 62 19
ssd@ow.ch
www.ow.ch

Gesetz zu technisch." In diesem Sinne ist in der Verordnung der Begriff Datei – anstelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

Abs. 2
In vielen Fällen kann der Informationsgehalt eines Dokuments im Format PDF rechtsgenüglich wiedergegeben werden. Insofern soll die Beilage in diesem weit verbreiteten Format eingereicht werden, was die Fallbearbeitung durch die Verfahrensbeteiligten erleichtert. Reichen die Verfahrensbeteiligte ihre Beilagen im Format PDF ein, entfällt die Konversion durch die Justizbehörden, allen Beteiligten liegt das gleiche Dokument vor. Die Digitalisierung soll die Verfahren beschleunigen und die Aktenführung vereinfachen. Wenn Dokumente im Regelfall als PDF-Dokument vorliegen, ermöglicht dies eine speditive Bearbeitung durch die Anwaltschaft und die Behörden. Geschäftsverwaltungssysteme der Anwältinnen, Anwälte und Behörden können aus Sicherheitsgründen nur mit einer beschränkten Anzahl an Dateitypen umgehen ('Whitelistening' von Fileformaten). Wenn das Format der Beilagen frei gewählt werden könnte, würde dies die Fallbearbeitung erheblich erschweren. Alle Verfahrensbeteiligten müssten zuerst nach dem passenden Programm suchen, um eine Datei zu öffnen. Zudem würde die uneingeschränkte Formatwahl ein erhebliches IT-Sicherheitsrisiko für alle Beteiligten darstellen.

In Einzelfällen kann das Format PDF den Informationsgehalt eines Dokuments nicht genügend wiedergeben. Zu denken ist beispielsweise an Audio oder Videoaufnahmen, an mehrspurige Tunnelüberwachungen oder Aufzeichnungen aus Elektroautos. Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattformen übermittelt werden können. Aus Sicherheitsgründen scannt die zentrale Plattform alle Dateien auf Viren. Dabei kann die zentrale Plattform grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Für Dokumente, welche nicht direkt über die Plattformen übermittelt werden dürfen, besteht die Möglichkeit zur Übermittlung in einem Container, beispielsweise als Zip-Format.

Welche Dateiformate die Plattformen verarbeiten müssen, ist durch das EJPD nach Anhörung der Betreiberin der zentralen Plattform in einer Departementsverordnung zu regeln.
Absatz 2 sollte daher wie folgt lauten:

Die Beilagen können in jedem Format übermittelt werden. Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden.

Abs. 3 und 4
Die vorgeschlagene Auswahl der Dateiformate wird begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen. Die Liste der unterstützten Dateiformate ist einem stetigen Wandel unterworfen. Es sind daher häufige Anpassungen zu erwarten. Zudem ist das reine Benennen von Formaten in der Verordnung nicht hinreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei dennoch verschlüsselten oder passwortgeschützten Elementen. Dies ist in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde
Im elektronischen Rechtsverkehr wird das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente vor der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben. Die Plattform dagegen bringt ihr Siegel nach der Übermittlung auf die Plattform auf der ausgestellten Eingangsquittung gestützt auf Artikel 5 an. Artikel 6 regelt die Sieglung der Dokumente durch die verfahrensleitende Behörde vor der Übermittlung über eine Plattform (Art. 22 Abs. 2 BEKJ). Der Vorentwurf führt aus, dass bei der Übermittlung von mehreren Dokumenten die Sieglung eines Dokuments genüge. Dies ist korrekt. Zu ergänzen ist, dass die Siegelung durch die verfahrensleitende Behörde unabhängig von der Anzahl der übermittelten Dokumente erfolgt. Auch ein einzelnes Dokument, welches die verfahrensleitende Behörde übermittelt, muss gesiegelt werden, damit die Authentizität des Dokuments unabhängig von einer Plattform überprüft werden kann.

Die Ausführungen im erläuternden Bericht, wonach eine Behörde alle Dokumente mit einem Siegel versehen muss, widersprechen dem Wortlaut der Verordnung: Die Siegelung eines Dokuments durch

die verfahrensleitende Behörde genügt. Zudem entspricht die Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden nicht dem technischen Konzept der zentralen Plattform.

Die Unterscheidung zwischen verfahrensleitenden und verfahrensbeteiligten Behörden ist für verschiedene Funktionalitäten der zentralen Plattform essenziell. Beispielsweise können nur verfahrensleitende Behörden Zustellungen vornehmen. Nur die Adresse von verfahrensleitenden Behörden ist für Drittpersonen aus dem öffentlichen Verzeichnis der zentralen Plattform ersichtlich. Würde an der Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden festgehalten, könnten alle Behörden uneingeschränkt und verfahrensunabhängig Zustellungen an andere Behörden, Organisationen und Privatpersonen vornehmen. Dies würde die zentrale Plattform für jegliche elektronische Kommunikation zwischen Behörden öffnen, wofür das BEKJ jedoch keine hinreichende gesetzliche Grundlage liefert. Sinn und Zweck des BEKJ ist es, die elektronische Kommunikation in Justizverfahren zu ermöglichen.

Nur verfahrensleitende Behörden sind verpflichtet, ihre Dokumente elektronisch zu siegeln. Artikel 22 Absatz 2 BEKJ ist daher einschränkend auszulegen. Das elektronische Siegel stellt die Herkunft, den Zeitpunkt, die Integrität und die Authentizität des gesiegelten Dokuments sicher. Die Verfügung oder der Entscheid einer verfahrensleitenden Behörde begründen Rechte und Pflichten und entfalten Wirkung über das einzelne Verfahren hinaus. Betroffene müssen daher unabhängig von einem konkreten Verfahren oder von der zentralen Plattform prüfen können, ob das fragliche Dokument integer und authentisch ist und von der dafür zuständigen Behörde erstellt wurde. Das elektronische Siegel ist zusammengefasst genau dort notwendig, wo Behörden autoritativ auftreten.

Verfahrensbeteiligte Behörden dagegen dürfen nicht verpflichtet werden, ihre Dokumente zu siegeln. Die Dokumente, welche verfahrensbeteiligte Behörden in einem Justizverfahren übermitteln, begründen in der Regel keine neuen Rechte und Pflichten. Typischerweise handelt es sich bei diesen Dokumenten um Auszüge aus bestehenden Registern, Auszüge aus bestehenden Akten früherer Verfahren, bereits eröffnete Verfügung oder Entscheide aus abgeschlossenen Verfahren, welche nun für ein Justizverfahren zur Verfügung gestellt werden. Die Authentifizierung auf der zentralen Plattform ermöglicht die korrekte Identifikation der Behörde. Will ein Verfahrensbeteiligter die Integrität oder Authentizität eines von einer verfahrensbeteiligten Behörde übermittelten Dokuments in Frage stellen, ist dies eine Frage der Beweiswürdigung im entsprechenden Verfahren.

Würde an der Siegelpflicht für alle Behörden gemäss erläuterndem Bericht festgehalten, so müssten alle Schweizer Behörden auf allen Stufen mit einem Siegel ausgestattet werden. Für die flächendeckende Ausstattung aller Schweizer Behörden mit einem elektronischen Siegel liefert das BEKJ keine genügende gesetzliche Grundlage. Für die Kantone wäre zudem eine flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden.

Gemäss erläuterndem Bericht müssen Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, nicht mehr gesiegelt werden. Diese Aussage entspricht nicht dem Konzept des BEKJ. Das BEKJ schreibt keine Funktionalität vor, wonach die zentrale Plattform qualifizierte elektronische Signaturen von Behördenmitgliedern einer Behörde zuordnet. Aus diesem Grund müssen verfahrensleitende Behörden Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, vor dem Versand über die Plattform standardmässig mit ihrem Siegel versehen. Es müsste hingegen geklärt werden, wie Behörden Dokumente unterzeichnen können.

Wichtig zu ergänzen ist die Unterscheidung zwischen Versand und Akteneinsicht. Bei der Akteneinsicht besteht, wie der erläuternde Bericht zu Artikel 7 ausführt, dagegen keine Pflicht zur Siegelung der Dokumente durch die verfahrensleitende Behörde.

Art. 7 Siegelung der Dokumente durch die Plattformen

Abs. 1

Der Grundsatz der Siegelung durch die Plattformen wird im Vorentwurf korrekt wiedergegeben: Träger des Siegels der Plattform ist die Quittung, nie das übermittelte Dokument. Im Falle der zentralen Plattform handelt es sich dabei um die sogenannte Eingangs oder Abrufquittung. Die zentrale Plattform siegelt die Quittungen der Benutzerinnen und Benutzer, unabhängig davon, ob sie ein oder mehrere Dokumente übermitteln. Absatz 1 sollte daher wie folgt lauten:

Werden ~~mehrere~~ Dokumente ~~zusammen~~ übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an. Das Dokumentmuss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.

Abs. 2
Absatz 1 beschreibt die Siegelung der Quittungen. Die Übermittlung von gesiegelten Dokumenten folgt den gleichen Regeln wie in Absatz 1. Absatz 2 muss daher gestrichen werden.

Art. 9 Profile
Abs. 2 Bst. b
Diese Bestimmung bezieht sich einzig auf verfahrensleitende Behörden, die auch im Adressverzeichnis der zentralen Plattform erscheinen. Bei verfahrensleitenden Behörden ist auf die Angabe einer postalischen Adresse zu verzichten, da eine Behörde über mehrere Standorte und verschiedene Postadressen verfügen kann. Bst. b ist entsprechend zu streichen.

Abs. 3 Bst. a
Die Übernahme des Geburtsdatums aus dem AGOV-Account wird insbesondere im Bereich Straf- und Verwaltungsrecht begrüsst. Zu betonen ist, dass die Privatadresse im AGOV-Account nicht aktualisiert wird. Die Richtigkeit der Privatadresse beruht auf der Selbstdeklaration der Nutzerin oder des Nutzers. Sie wird anlässlich der Identifikation nicht geprüft, weshalb sie nicht verlässlich ist. Auch aus Sicht des Datenschutzes ist die Speicherung der Privatadresse in den Benutzerprofilen als kritisch zu betrachten. In den Profilen der natürlichen Personen sollte daher auf die Erhebung von Postadressen verzichtet werden.

Abs. 3 Bst. b
Unternehmen haben verschiedene Strukturen und verschiedene Niederlassungen, weshalb das verwendete digitale Profil nicht mit der Postadresse übereinstimmen muss. Die Postadresse bringt beim digitalen Zustellen daher keinen nennenswerten Mehrwert. Auch bei Organisationen soll daher auf die Postadresse verzichtet werden.

Abs. 4
Der Sinn von Absatz 4 ist nicht verständlich. Es ist unklar, ob sich die Pflicht zur elektronischen Übermittlung auf die natürliche Person oder die Organisation, für welche die natürliche Person tätig ist, Bezug nimmt. Letzteres dürfte der Fall sein. Die Formulierung von Absatz 4 ist dementsprechend zu präzisieren. Im erläuternden Bericht wird die verantwortliche Person einer Organisation erwähnt. Es ist wünschenswert, dass die Rolle der verantwortlichen Person in Bezug auf die zentrale Plattform in der Verordnung geklärt wird.

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen
Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein "Briefkasten" und keine Langzeitablage sein soll. Bei den Quittungen scheint es dagegen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Natürlich müssen die Behörden darum besorgt sein, die Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch aufgrund der Funktionsweise der zentralen Plattform – etwa im Fall von Zustellungen – dazu kommen, dass das Herunterladen der Quittungen unterbleibt. Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von der Plattform selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen.

Quittungen können Personendaten enthalten (so etwa die Namen von Verfahrensbeteiligten), was diese im Kontext von Justizverfahren unter Umständen zu besonders schützenswerten Personendaten macht. Jedoch sind diese Daten, wie auch die weitaus sensibleren Aktenstücke selbst, auf der Plattform verschlüsselt gespeichert. Hinzu kommt, dass es sich bei Quittungen um sehr kleine Datenmengen handelt, die keinen hohen zusätzlichen Speicherbedarf verursachen, selbst wenn sie lange auf der Plattform verfügbar bleiben müssen.

In Anlehnung an die Zeitspanne von drei Jahren, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind, wird vorgeschlagen, Artikel 12 wie folgt zu ändern, respektive zu ergänzen:

1 Die auf einer Plattform gespeicherten Dokumente ~~und Quittungen~~ werden sechs Monate nach der Entgegennahme ~~beziehungsweise nach der Erstellung~~ automatisch vernichtet.
2 Stehen Dokumente zur Akteneinsicht zur Verfügung, so bestimmt die verfahrensleitende Behörde, wie lange die Dokumente auf der Plattform abrufbar sind. Nach Ablauf der Frist werden die Dokumente automatisch ~~vernichtet~~ gelöscht.
3 Quittungen werden drei Jahre nach ihrer Erstellung automatisch gelöscht.

Art. 16 Aufteilung der Gebühr
Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 Prozent wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die Aufteilung der Gebühr sollte Gegenstand der Prüfung sein.

Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen. Anhand dieser verbindlichen Angaben legt das EJPD den jährlichen Gebührenbeitrag fest; es berücksichtig dabei die in Artikel 15 Absatz 4 definierten Schwellenwerte und den allfälligen Beitritt eines Nichtmitgliedes zur Körperschaft justitia.swiss nach deren Gründung.
Vorgeschlagen wird folgender Wortlaut:

(…)
2 Der Anteil der Kantone wird ~~gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt~~ unter den Kantonen, die Mitglieder der öffentlich-rechtlichen Körperschaft sind, proportional zu deren ständigen Wohnbevölkerung am 1. Januar des Vorvorjahres, für das die Gebühr fällig wird, verteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen ~~im Zeitpunkt der Festlegung nach Artikel 15~~.

3 Das EJPD legt jährlich die Verteilung der Gebühr auf die Kantone fest.

Art. 22a (neu) Rücksendung von physischen Dokumenten
In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7) wird dargelegt, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Artikel 30 BEKJ in die vorliegende Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe.

Diese Feststellung bezieht sich auf die Auslegung des in Artikel 30 BEKJ enthaltenen Begriffs der "Dokumente", der im Gesetz weder weiter nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird. Eine differenzierende Betrachtung ist nach hier vertretener Auffassung aber erforderlich, um mit einer lückenhaften Verordnung zum BEKJ keine Probleme zu schaffen, die es in der analogen Welt noch gar nicht gibt. Damit ist auch gesagt, dass die anwendbaren Prozessgesetze nach hier vertretener Meinung durchaus Raum für eine Auslegung der Bestimmungen des BEKJ im Sinne ihrer gesetzgeberischen Zielsetzung lassen.

Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen in Papierform eingehen, weil derlei Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien

rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ entgegen den Erläuterungen zum Vorentwurf nicht restriktiv ausgelegt, schafft das Gesetz zur Einführung des elektronischen Rechtsverkehrs neue Rücksendungspflichten im Papierprozess, die es bisher in der analogen Welt nicht gab. Dies kann nicht der Willen des Gesetzgebers gewesen sein. Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft, die im Schriftstück enthalten ist. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden überwiegend weggeworfen werden, sobald sie wieder bei ihren ursprünglichen Absenderinnen und Absendern eingetroffen sind.

Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, könnte mit den zurückgeschickten Dokumenten nicht Beweis geführt werden, weil sich nicht feststellen liesse, ob es auch diese Papiere waren, die gegenüber der Behörde eingereicht worden waren. Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Artikel 30 Absatz 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Der Botschaft zum BEKJ ist zu entnehmen, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen. Damit ist auch gesagt, dass die Rücksendepflicht von Urkunden, an deren Wiedererhalt die Absenderinnen und Absender ein Interesse haben, vorliegend nicht in Frage gestellt wird.

Hingegen braucht nicht weiter ausgeführt werden, dass durch die Auslegung des BEKJ im Sinne eines neu geschaffenen, replizierenden Postverkehrs in Papierform ein enormer Mehraufwand durch Porti und Arbeitsaufwand geschaffen wird. Eine Gesetzesauslegung, die letztlich dazu führt, dass tausende von Altpapierbündeln mit Porto versehen werden müssen, kann nicht von der gesetzgeberischen Absicht getragen sein.

Aus den oben genannten Gründen wird vorgeschlagen, einen neuen Artikel 22a einzufügen. Die gewählte Formulierung stellt klar, dass Dokumente, die gemäss Artikel 30 Absatz 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Artikel 30 BEKJ in die Verordnung zu schreiben. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen:

2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten
[...]
Art. 22a Rücksendung von physischen Dokumenten
Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.

Art. 22b (neu) Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7 f.) wird ausgeführt, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Artikel 353 Absatz 1 Buchstabe k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: "Der Strafbefehl enthält: (...) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird." Artikel 238 Buchstabe h nZPO enthält eine ähnliche Regelung für zivilgerichtliche Entscheide.

Artikel 22 konkretisiert Artikel 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ zwar die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird.

Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von zehn bis zwanzig Prozent der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Zwar liegt dem BEKJ als Regulierungsgrundsatz die Idee zugrunde, dass Privatpersonen nicht zur elektronischen Kommunikation mit den Behörden gezwungen werden sollen und an dieser Grundlage soll vorliegend deshalb auch nicht gerüttelt werden. Hingegen kann es nicht richtig sein, das Unterschriftserfordernis derart restriktiv auszulegen, dass jeglichem Fortschritt ein Riegel vorgeschoben wird.

Artikel 22 Absatz 2 BEKJ ist zu entnehmen, dass künftig mittels eines geregelten elektronischen Siegels sichergestellt werden soll, dass ein elektronisch erstelltes Dokument tatsächlich von der zuständigen Behörde stammt, die sich etwa aus dem Briefkopf o.ä. ergibt. Zu diesem Artikel ist der Botschaft zum BEKJ zu entnehmen: "Das Unterschriftserfordernis stellt bei der Digitalisierung oft ein Hindernis dar. Anstelle der Unterschrift sieht das Gesetz die Authentifizierung mit Hilfe eines anerkannten elektronischen Identitätsnachweises sowie dem Anbringen eines geregelten elektronischen Siegels vor." Damit ist gesagt, dass das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift ersetzt. Für einen Rückgriff auf Artikel 14 OR bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel

Zwar ist dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens insoweit beizupflichten, dass den massgeblichen Verfahrensgesetzen zu entnehmen ist, dass etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Nach hier vertretener Auffassung lässt diese Formulierung aber durchaus eine Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes zu.

Bereits heute ist es absolut gängige Praxis bei den Zivilgerichten und den Strafbehörden, das Original der Endentscheide zu den Akten der Behörde zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen. Wie schon weiter oben zur Bestimmung über den Rückversand eingesandter Papierdokumente ausgeführt, wird nun durch den Verzicht auf eine reduzierende Auslegung eine neue Pflicht in der analogen Welt geschaffen. Wird dem erläuternden Bericht gefolgt, soll es plötzlich eine Pflicht zum Versand von Papieroriginalen geben. Damit wird der Versand von Papieroriginalen in der digitalen Welt exponentiell vervielfacht. Das kann nicht die Idee der Gesetzgebung gewesen sein. Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Einer Papierkopie des elektronischen Originals kommt exakt derselbe Informationsgehalt zu wie ein Entscheid, der eine handschriftliche Signatur trägt. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann.

Die vorgeschlagene Lösung hätte den Vorteil, dass in einem Verfahren keine zwei Originale desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids

(ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG stellt für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Aus den genannten Gründen wird deshalb vorgeschlagen, einen neuen Artikel 22b einzufügen:

Art. 22b Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten
Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Originalkostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.

Sollte an der viel zu engen Auslegung des BEKJ festgehalten werden, die im erläuternden Bericht skizziert ist, wäre zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen, um dem in den Verfahrensgesetzen verwendeten Begriff der "Unterschrift" genüge zu tun, obwohl diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung durch das Behördensiegel ersetzt wurde.

Art. 24 Elektronische Übermittlung unter Behörden
Nach unserer Einschätzung ist die Sachüberschrift zu weit gefasst und daher irreführend. Es handelt sich stets um die Kommunikation von und zu Strafbehörden oder Zivilgerichten im Rahmen von Verfahren nach StPO oder ZPO. Gleichzeitig erscheint es erforderlich, den Begriff der übrigen Behörden, die mit den Strafbehörden elektronisch kommunizieren zu müssen, zu definieren. Insbesondere mit Blick auf öffentlich-rechtliche Körperschaften, die nicht hoheitlich handeln, besteht insoweit Unklarheit.

Diese Bestimmung konkretisiert die Ausnahmen von Artikel 128c Absatz 2 der Zivilprozessordnung, Artikel 103c Absatz 2 der Strafprozessordnung und Artikel 8d Absatz 2 des Opferhilfegesetzes. Diese Ausnahmen sind dort sinnvoll, wo in Zivil- oder Strafverfahren eine grosse Anzahl von Kommunikationen mit Behörden anfallen, die nicht Teil der Straf- oder Zivilprozesskette sind und wo eine direkte Kommunikation, z.B. über eine Schnittstelle, etwa zur Weitergabe von Metadaten oder aus Kostengründen dem Rechtsverkehr über die Plattform vorzuziehen ist. Zu denken ist im Strafprozess etwa an Steuer oder Migrationsbehörden oder auch an grosse Verkehrsbetriebe oder rechtsmedizinische Institute, die auch unter den Behördenbegriff fallen dürften. Ebenso bestimmte Behörden des Bundes wie das BAZG.

Die Voraussetzungen sollten sich an Artikel 23 orientieren und nicht darüber hinausgehen. Es ist jedenfalls nicht ersichtlich, weshalb Artikel 24 strengere Anforderungen vorsieht, da Artikel 103c Absatz 2 der Strafprozessordnung – anders als Art. 103b Absatz 2 mit der Feststellung der Zeitpunkte der Übermittlung und dem Schutz der Akte vor Veränderung und unberechtigter Kenntnisnahme überhaupt keine Anforderungen an die Dokumentation einer Übermittlung stellt.

Art. 28 Inkrafttreten
Die Finanzierung des Projekts Justitia 4.0, welches die zentrale Plattform im Auftrag der Kantone, des Bundes und der Justizbehörden aufbaut, ist bis Ende Jahr 2027 gesichert. Die Finanzierung von Betrieb und Weiterentwicklung der zentralen Plattform muss daher spätestens ab Anfang 2028 über Gebühren erfolgen. Die Verordnung muss gleichzeitig mit dem abschliessenden Inkrafttreten des BEKJ in Kraft gesetzt werden.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Christoph Amstad
Regierungsrat

Kopie an:
- Kantonale Mitglieder der Bundesversammlung
- Amt für Justiz
- Staatsanwaltschaft
- Kantonspolizei
- Gerichte
- Staatskanzlei

Kanton Schaffhausen
Volkswirtschaftsdepartement
Mühlentalstrasse 105
CH-8200 Schaffhausen
www.sh.ch

Telefon 052 632 73 80
dino.tamagni@sh.ch

Volkswirtschaftsdepartement

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per E-Mail an cornelia.perler@bj.admin.ch

Schaffhausen, 11. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Stellungnahme

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie dem Kanton Schaffhausen den Entwurf in obgenannter Angelegenheit zur Vernehmlassung unterbreitet. Wir bedanken uns für diese Möglichkeit und nehmen gerne wie folgt zum Entwurf Stellung:

Ingress:

Die Delegationsbestimmungen im Ingress des VE-VEKJ sind unvollständig und sollten ergänzt werden, auch wenn dies zu einem längeren Ingress führt.

Art. 2:

Aufgrund der schnellen technischen Entwicklung sollte die maximale Dateigrösse gemäss Abs. 1 lit. c in einem Anhang zur Verordnung oder in eine Departementsverordnung des EJPD geregelt werden statt in der VEKJ. Dadurch wird eine hinreichende Flexibilität gewährleistet.

Art. 4:

Abs. 2:

Auch Beilagen sollten grundsätzlich im PDF- oder PDF/A-Format eingereicht werden. Wenn das Format der Beilagen frei gewählt werden kann, wie in Abs. 2 vorgesehen, ist mit einem erheblichen Bearbeitungsaufwand zu rechnen, da Verfahrensbeteiligte jeweils nach einem Programm suchen müssen, welches das Format öffnen kann. Zudem würde eine uneingeschränkte Formatwahl ein erhebliches Sicherheitsrisiko für alle Beteiligten darstellen.

Es gibt Fälle, in welchen die Formate PDF bzw. PDF/A den Informationsgehalt eines Dokuments nicht genügend wiedergeben können (z.B. Audio- oder Videodateien). Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattform übermittelt werden können.
Wir schlagen folgende Formulierung vor: "Ist das Format PDF ungeeignet, den Inhalt einer Beilage korrekt wiederzugeben, kann diese im Originalformat übermittelt werden."

Abs. 3 und 4:
Die vorgeschlagene Auswahl der Dateiformate wird begrüsst. Es stellt sich allerdings die Frage, ob aufgrund des schnellen technischen Wandels die Dateiformate nicht besser in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD bestimmt werden sollen.

Art. 5 Abs. 2 lit. d Ziff. 2:
Diese Bestimmung präzisiert, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung auszuweisen bzw. aufzulisten sind. Dies ist nicht möglich: Nicht übermittelte Dokumente können auf der Eingangsquittung nicht aufgeführt werden, da diese eben *nicht* übermittelt wurden. Die Quittung kann keine Hashwerte von Dateien enthalten, welche nicht übermittelt worden sind. Kann die Plattform ein oder mehrere Dokumente nicht übermitteln, so erhält die Absenderin oder der Absender eine Mitteilung der Plattform, jedoch keine Quittung. Art. 5 Abs. 2 lit. d Ziff. 2 ist daher zu streichen.

Art. 6:
Durch eine zu weite Auslegung von Art. 22 Abs. 2 BEKJ könnten *sämtliche* Behörden zur Siegelung aller Eingaben an die Strafbehörden gezwungen werden (beispielsweise die Steuerverwaltung, wenn sie der Staatsanwaltschaft Auskunft über die finanziellen Verhältnisse einer Person erteilt). Dies erscheint wenig zielführend. Die Sieglung eines Dokuments durch die verfahrensleitende Behörde genügt. Verfahrensbeteiligte Behörden sollen hingegen nicht verpflichtet werden, Dokumente zu siegeln.
Es muss geklärt werden, wie mit Dokumenten umgegangen werden soll, welche gemäss gegenwärtiger Rechtsprechung eine Unterschrift der Autorenschaft tragen müssen, beispielsweise Sachverständigengutachten (z.B. Gutachten des rechtsmedizinischen Instituts). Diese können durchaus von Behörden bzw. Amtsstellen erbracht werden. In diesen Fällen ist es erheblich, welche sachverständige Person das Gutachten erstattet hat.

Art. 7:
Abs. 1:
Träger des Siegels der Plattform ist die Quittung und nie das übermittelte Dokument. Die Plattform siegelt die Quittungen der Benutzerinnen und Benutzer unabhängig davon, ob sie ein oder

mehrere Dokumente übermitteln. Somit empfehlen wir folgende Anpasung: "Werden ~~mehrere~~ Dokumente übermittelt […]".

Art. 12:

Quittungen und Dokumente sollen gemäss VE-VEKJ maximal 6 Monate aufbewahrt werden. Diese Frist ist zu kurz. Gerade Quittungen können erst sehr spät im Verfahren noch benötigt werden, um etwa die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Wir schlagen daher eine Verlängerung der Frist auf drei Jahre vor. Dies entspricht der Frist, welche auch die Post für Nachforschungsaufträge kennt.

Art. 22:

<u>Rücksendung von physischen Dokumenten:</u>

In Art. 30 BEKJ ist eine Rücksendepflicht für "Dokumente" vorgesehen. Gerade in Strafprozessen werden physisch eingereichte Dokumente jedoch heute nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei der Polizei und der Staatsanwaltschaft werden etwa auch nach Inkrafttreten der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen in Papierform eingehen, weil diese in der Regel von Privatpersonen stammen, die sich nicht zuerst auf der Plattform registrieren wollen. Diese riesige Menge an Eingaben wird für die Strafbehörden geschrieben und oft mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Originale verbleiben meist bei der Absenderin oder dem Absender.

Wird das BEKJ so ausgelegt, dass auch solche "Dokumente" zurückgesendet werden sollen, entsteht dadurch im Vergleich zu heute ein erheblicher Mehraufwand sowohl zeitlich, als auch finanziell. Dies obwohl der Rückversand solcher Dokumente bereits heute nicht erfolgt und im Übrigen keinerlei Nutzen hat. Es sollte daher in der Verordnung unterschieden werden zwischen "einfachen Mitteilungen" und "Dokumenten". Es kann nicht das Ziel von Justitia 4.0 sein, den Arbeitsaufwand für die Behörden künstlich erheblich zu erhöhen.

<u>Trägerwandel:</u>

Gemäss Ziffer 2.6 des erläuternden Berichts wurde die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, verworfen, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen (z.B. Art. 80 Abs. 2 StPO "Entscheide ergehen schriftlich […]. Erfolgt die Zustellung auf Papier, so werden sie von der Verfahrensleitung sowie der protokollführenden Person unterzeichnet; Art. 353 Abs. 1 lit. k nStPO: "Der Strafbefehl enthält […] die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.").

Art. 22 VE-VEKJ konkretisiert Art. 29 BEKJ und damit den Trägerwandel von Papiereingaben zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um sehr gewichtige Anforderungen handelt. Standard soll gemäss Grundkonzept des BEKJ die elektronische Aktenerstellung sein. Nur wo sich Private nicht auf einer elektronischen Plattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird. Gerade Übertretungsstrafbehörden und Staatsanwaltschaften erlassen jedes Jahr sehr viele Strafbefehle. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss Auslegung des BEKJ auf Wunsch der Privaten doch wieder in Papierform geführt werden müssen, würden nur wenige Dossiers elektronisch geführt werden können.
Dies entspricht nicht dem Wunsch, dass künftig in der Schweizer Justiz das digitale Primat gelten soll. Es ist zwar richtig, dass Privatpersonen nicht zur elektronischen Kommunikation gezwungen werden sollen, allerdings sollte dies nicht derart restriktiv ausgelegt werden, dass der digitale Fortschritt verhindert wird.

Es sollen daher stets nur Papierkopien des elektronischen Originals versendet werden, z.B. bei Strafbefehlen. Sollte die Kopie allein nicht genügen, so könnte allenfalls mit einem Beglaubigungsstempel gearbeitet werden, mit welchem die Verfahrensleitung sowie die protokollführende Person bzw. die ausstellende Person unterschriftlich bestätigt, dass die Kopie mit dem elektronischen Original übereinstimmt. Sollte die Empfängerin oder der Empfänger dennoch Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann. Es ist sicherzustellen, dass es nicht plötzlich zwei verschiedene Originale gibt.

Unseres Erachtens sollte im Übrigen zeitnah die StPO angepasst werden, sodass künftig die Beglaubigung von Kopien elektronischer Originale auch durch das Sekretariat der Strafbehörde erfolgen kann.

Art. 23:
Art. 23 VE-VEKJ bezieht sich auf nArt. 128b Abs. 2 und 3 ZPO, nArt. 103b Abs. 2 und 3 StPO sowie nArt. 8c Abs. 2 und 3 OHG. In diesem Artikel geht es um die Weitergabe von Akten zwischen den Behörden, z.B. bei einem Weiterzug an eine übergeordnete Instanz, wenn andere Behörden mit bestimmten Verfahrenshandlungen beauftragt werden (z.B. Ermittlungsauftrag von der Staatsanwaltschaft an die Kriminalpolizei) oder bei der Übermittlung von Ergebnissen von Untersuchungshandlungen, welche die Polizei an die Staatsanwaltschaft übermittelt. Bei

der elektronischen Weitergabe von Akten zwischen den Strafbehörden oder innerhalb des Kantons sollten andere Anforderungen gelten als bei der Kommunikation über die zentrale Plattform, beispielsweise durch Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank. Artikel 23 sollte so angepasst werden, dass auch eine Weitergabe mittels Mutation von Zugriffsrechten zulässig ist.

Art. 24:

Dieser Artikel regelt, dass eine Zustellung unter Behörden, einschliesslich Gerichten und Amtsstellen ausserhalb der Plattform nach dem BEKJ erfolgen können. Es ist unklar, wie diese Bestimmung von der im BEKJ vorgesehenen Pflicht zur Nutzung der Plattform justitia.swiss durch die "übrigen Behörden" abzugrenzen ist. Allenfalls ist der Begriff "Behörden" genauer zu definieren.

Inkraftsetzung:

Die Inkraftsetzung der VEKJ ist auf Q2 2027 vorgesehen. Aufgrund der zahlreichen organisatorischen Anpassungen ist auf eine hinreichende Planungssicherheit zu achten.

Abschliessende Bemerkungen:

Nutzung von PrivaSphere und IncaMail in hängigen Verfahren

Im erläuternden Bericht wird die Auffassung vertreten, dass die bisherigen anerkannten Zustellplattformen (PrivaSphere Secure Messaging und IncaMail) weiterhin benutzt werden könnten in Verfahren, welche beim abschliessenden Inkrafttreten des BEKJ bereits hängig waren. Die Übergangsbestimmungen in den Prozessgesetzen würden dies ermöglichen (Erläuternder Bericht, S. 8). Unseres Erachtens trifft dies nicht zu, da der Grundsatz der unmittelbaren Anwendbarkeit neuer verfahrensrechtlicher Regelungen gilt. Neue verfahrensrechtliche Regelungen gelangen mithin grundsätzlich mit ihrem Inkrafttreten auch auf bereits hängige Verfahren zur Anwendung. Das Übergangsrecht bezieht sich auf den Erlass der ZPO bzw. der StPO und gilt für nachträgliche Teilrevisionen an den Prozessgesetzen nicht.

Selbst wenn aber das Übergangsrecht gelten sollte, so würde dies voraussetzen, dass der Bundesrat weiterhin eine Liste der anerkannten Zustellplattformen führen müsste. Es muss sichergestellt werden, dass es sich bei den Zustellplattformen auch weiterhin um anerkannte Zustellplattformen handelt, welche die in der VeÜ-ZSSV geregelten Anforderungen erfüllen.

Wir regen an, den Bericht entsprechend anzupassen und festzuhalten, dass die elektronische Kommunikation ab Inkrafttreten des BEKJ nur noch über die Plattform justitia.swiss und nicht mehr über die bisherigen Plattformen (PrivaSphere Secure Messaging oder IncaMail) erfolgen kann.

Nutzerkreis der Plattform justitia.swiss

Derzeit ist vorgesehen, dass die Plattform justitia.swiss zwar für verwaltungs*gerichtliche* Verfahren genutzt werden kann, nicht jedoch für Verwaltungsverfahren. Dies wird unter anderem dazu führen, dass in gewissen Verfahren je nach Verfahrensstadium die Plattform genutzt werden kann oder nicht, was für Verwirrung insbesondere unter den Privaten sorgen dürfte.

Die Staatsanwaltschaft führt beispielsweise nicht nur Strafverfahren, sondern auch Verwaltungsverfahren: Während dem Verfahren richtet sich die Einsicht in Strafakten nach Art. 101 StPO und damit erfolgt die Akteneinsicht über die Plattform justitia.swiss. Ist ein Verfahren abgeschlossen, richtet sich die Einsicht nach dem kantonalen Verwaltungsrecht, womit hierfür die Plattform justitia.swiss nicht benützt werden kann. Wir sind daher der Ansicht, dass die Nutzung der Plattform auch für Verwaltungsverfahren zugelassen werden sollte.

Für die Kenntnisnahme und Berücksichtigung unserer Stellungnahme danken wir Ihnen.

Freundliche Grüsse

Volkswirtschaftsdepartement
Der Vorsteher:

D. Tamagni

Dino Tamagni
Regierungsrat

z. K.
– Departement des Innern
– Finanzdepartement
– Obergericht

Regierungsrat des Kantons Schwyz

VERSENDET AM 16. JUNI 2026

kantonschwyz

6431 Schwyz, Postfach 1260

per E-Mail

Eidgenössisches Justiz- und
Polizeidepartement EJPD
3003 Bern

cornelia.perler@bj.admin.ch

Schwyz, 9. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren
Vernehmlassung des Kantons Schwyz

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 13. März 2026 hat das Eidgenössische Justiz- und Polizeidepartement EJPD den Kantonsregierungen die Unterlagen zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) zur Vernehmlassung bis 22. Juni 2026 unterbreitet. Dafür bedanken wir uns.

Der Vorentwurf hat zum Ziel, das Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz vom 20. Dezember 2024 (BEKJ, SR 172.023) umzusetzen.

Der Kanton Schwyz stimmt dem Vorentwurf mit nachstehenden Hinweisen zu.

Gemäss Art. 2 Abs. 1 Bst. c E-VEKJ müssen die Plattformen zusätzlich zu den Anforderungen gemäss BEKJ in der Lage sein, bis zu zwei Gigabyte grosse Dokumente entgegenzunehmen und übermitteln zu können. Obschon die wenigsten Dateien in der Grössenordnung von mehr als zwei Gigabyte sein dürften und mit Zip / 7-Zip eine Komprimierungslösung besteht, werden in den kantonalen Webtransfer-Systemen teilweise Dateiobergrenzen von mehr als zwei Gigabyte angeboten. Der Kanton Schwyz beantragt deshalb, folgenden Wortlaut zu benutzen: «Die Plattform muss mindestens zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln können.» In der Praxis ist regelmässig mit Dateien zu rechnen, die zwei Gigabyte bei weitem übersteigen werden. Verschiedene Kantone prüfen derzeit die Möglichkeit, umfangreiche Daten nicht auf die Plattform zu laden, sondern an einem anderen Ort zu speichern und einen externen Zugriff zu ermöglichen. Bei sehr grossen Datenmengen ist dieser Weg unumgänglich. Aus Sicht des Kantons Schwyz wäre zielführend, wenn die öffentlich-rechtliche Körperschaft justitia.swiss die Kantone in diesem Bereich koordinierend unterstützen könnte.

Art. 4 Abs. 1 E-VEKJ erwähnt «verfahrensleitende» und die «verfahrensbeteiligten Behörden», ohne jedoch diese Begriffe zu erläutern. Gerade auch wegen der anzustrebenden Ausweitung des Anwendungsbereichs über die Justiz hinaus auf Verwaltungsbehörden erscheint unklar, ob davon allgemein «Amtsstellen» oder nur eigentliche Behörden im engeren Sinn erfasst sein sollen. Aber auch im Bereich der Strafverfolgung ist unklar, ob namentlich Institute oder andere Stellen, die regelmässig ein Verfahren eingebunden werden, als «Behörden» gelten sollen. Aus Sicht des Kantons Schwyz ist der Entwurf diesbezüglich zu konkretisieren und der Geltungsbereich explizit zu regeln.

Gemäss Art. 4 Abs. 3 E-VEKJ muss die verfahrensleitende Behörde bestimmte Formate bearbeiten können. Der Kanton Schwyz regt an, die Aufzählung der Formate in einem Anhang zur Verordnung zu regeln, damit auf technische Entwicklungen in diesem Bereich schnell reagiert werden könnte.

Gemäss Art. 5 Abs. 1 E-VEKJ erstellt die Plattform eine einzelne Quittung, wenn mehrere Dokumente zusammen übermittelt werden. Unseres Erachtens sollte anstelle von «einzelne Quittung» der Begriff «einzige Quittung» verwendet werden.

Art. 10 E-VEKJ regelt den technischen Zugang über eine Schnittstelle. Um Unklarheiten zu vermeiden, wäre es aus Sicht des Kantons Schwyz eine Überlegung wert, den Titel von «Schnittstelle» in «Berechtigung via Schnittstelle» zu ändern.

Art. 16 E-VEKJ regelt die Aufteilung der Gebühr für die Nutzung der zentralen Plattform. Dass die Aufteilung gemäss ständiger Wohnbevölkerung erfolgt (Art. 16 Abs. 2 E-VEKJ) ist nicht zu beanstanden. Der grundsätzlichen Aufteilung (Bundesverwaltung und Bundesanwaltschaft 5 Prozent, Eidgenössische Gerichte 5 Prozent, Kantone 90 Prozent) liegt ein längerer Abklärungsprozess zugrunde. Dennoch regt der Kanton Schwyz an, in Art. 16 E-VEKJ festzulegen, dass die Anteile der Bundesverwaltung / der Bundesanwaltschaft und der Eidgenössischen Gerichte je mindestes fünf Prozent betragen und die Aufteilung aufgrund der Nutzungsdaten alle zehn Jahre überprüft wird.

Abschliessend noch eine redaktionelle Anmerkung: Bei Art. 3 Abs.1, Art. 8 Abs. 1 und 2 sowie bei Art. 13 E-VEKJ müsste nach «Artikel 1» jeweils noch «Absatz 1» eingefügt werden.

Für die abschliessende Inkraftsetzung des BEKJ sowie der VEKJ ist als frühestmöglicher Zeitpunkt der 1. Januar 2027 vorgesehen. Diese abschliessende Inkraftsetzung löst die Übergangsfristen nach Art. 37 BEKJ betreffend das Obligatorium aus. Aus Sicht der Kantons Schwyz kann einer Inkraftsetzung per 1. Januar 2027 zugestimmt werden.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Herr Bundesrat, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:

Michael Stähli
Landammann

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber

Regierungsrat

Rathaus

Barfüssergasse 24

4509 Solothurn

so.ch

Eidgenössisches Justiz- und
Polizeidepartement EJPD

3003 Bern

Per E-Mail an:

cornelia.perler@bj.admin.ch

22. Juni 2026

Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)
Stellungnahme des Kantons Solothurn

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie uns Gelegenheit eingeräumt, zum Vorentwurf betreffend Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VE-VEKJ) Stellung zu nehmen. Wir danken für diese Gelegenheit und reichen Ihnen fristgerecht unsere Stellungnahme ein.

1. Zu den einzelnen Bestimmungen

1.1. Zu Art. 2 Abs. 1 (Anforderungen an die Plattformen)

Gemäss Art. 2 Abs. 1 lit. a und lit. b muss eine Plattform für den Erhalt einer Betriebsbewilligung lediglich rudimentäre Anforderungen an die Informationssicherheit und den Datenschutz erfüllen. Später wird in Art. 13 festgehalten, dass sich die Datensicherheit der nach Art. 1 Abs. 1 lit. b von den Kantonen zur Verfügung gestellten Plattformen nach dem 3. Abschnitt des Informationssicherheitsgesetzes (ISG) und Art. 8 des Datenschutzgesetzes auszurichten haben. Dies muss für alle anderen Plattformen nach Art. 1 gelten und unseres Erachtens darf nicht stillschweigend davon ausgegangen werden, dass wie im erläuternden Bericht für Art. 13 beschrieben «vorliegende Bestimmung […] nur für die Kantone von Bedeutung [ist], da für den Bund die Vorgaben nach dem ISG ohnehin anwendbar sind.» Bei der Körperschaft handelt es sich um eine öffentlich-rechtliche Organisation, welche unseres Erachtens über Art. 2 ISG weder explizit als verpflichtete Behörde noch als Organisation aufgelistet ist. Auch handelt es sich bei der Plattform kaum um eine «kritische Infrastruktur» gemäss Art. 2 Abs. 5 ISG.

Antrag

Es ist - um Missverständnisse zu vermeiden - klar festzuhalten, dass die Anforderungen in Bezug auf die Sicherheit und den Datenschutz für jede Plattform gem. Art. 1 identisch sind.

Weiter zeigt die Erfahrung, dass die über Art. 2 Abs. 1 lit. c vorgesehene Obergrenze pro Dokument (2 GB) nicht ausreicht. In Justizverfahren werden die Dateien laufend grösser, dies entgegen der Feststellung im erläuternden Bericht, dass die Beschränkung der Dateigrösse in den allermeisten Fällen ausreichend sein sollte.

Antrag

Die in Art. 2 Abs. 1 lit c genannte Obergrenze von 2 GB ist anzuheben, muss aber nicht zwingend in der Verordnung festgehalten werden.

Wie im erläuternden Bericht beschrieben, werden die Dokumente und Quittungen nicht wie unter Art. 2 Abs. 1 lit. d beschrieben gelöscht, sondern es wird lediglich der Zugriff deaktiviert. Uns erschliesst sich die Aufzählung einer konkreten, einzelnen funktionalen Anforderung über die Verordnung nicht, zumal die Formulierung den Nutzenden eine falsche Tatsache suggeriert.

Antrag

Abs. 1 ist wie folgt zu formulieren:

[1]Die Plattformen müssen zusätzlich zu den Anforderungen nach dem BEKJ die ~~folgenden~~ Anforderungen **an die Informations- und Datensicherheit nach dem 3. Abschnitt des Informationssicherheitsgesetzes vom 18. Dezember 2020 und Art. 8 des Datenschutzgesetzes vom 25. September 2020** erfüllen.~~:~~

~~a. Die Dokumente sind vor unberechtigtem Zugriff und unberechtigter Änderung durch Dritte geschützt.~~

~~b. Die Dokumente auf der Plattform werden nach den technischen Standards der Bundesverwaltung verschlüsselt; sie werde verschlüsselt übermittelt.~~

~~c. Die Plattform kann bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln.~~

~~d. Die Benutzerinnen und Benutzer können die im Benutzerkonto ihres Profils enthaltenen Dokumente und Quittungen jederzeit löschen.~~

1.2. Zu Art. 3 Abs. 4 (Bewilligungsverfahren)

Im erläuternden Bericht wird zwar erwähnt, dass das EJPD nach erteilter Betriebsbewilligung regelmässig überprüfen muss, dass eine Plattform auch im laufenden Betrieb die notwendigen Voraussetzungen erfüllt. Dies wird über das VE-VEKJ nicht explizit verlangt und es kommt insbesondere nicht hervor, wer die Betriebsverantwortung einer Plattform nach BEKJ trägt. Die Verantwortlichkeit für den Betrieb einer Plattform nach BEKJ ist zwingend zu definieren und obliegt unseres Erachtens dem EJPD über die Erteilung und regelmässige Überprüfung der Betriebsbewilligung.

Antrag

[4]**Das EJPD überprüft nach erteilter Betriebsbewilligung regelmässig, ob eine Plattform die damit verbundenen Voraussetzungen weiterhin erfüllt.** Es entzieht die Bewilligung, wenn es feststellt, dass die Anforderungen nach Art. 2 und 25 BEKJ nicht mehr erfüllt sind.

1.3. Zu Art. 4 Abs. 2 (Format der Dokumente)

Gem. VE-VEKJ sollen die Beilagen in jedem Format übermittelt werden dürfen. Dies ist weder notwendig noch zielführend. Übermittelt werden dürfen nur zumindest langzeitaufbewahrungsfähige Formate und wie im erläuternden Bericht korrekt erwähnt, sollten auch die Beilagen wann immer möglich und sinnvoll im Format PDF oder PDF/A übermittelt werden. Dies ist auch im VE-VEKJ so zu präzisieren.

Zu beachten ist, dass es sich bei den erwähnten Formaten ZIP und 7z nicht um «Archivdateien» handelt, sondern im vorliegenden Kontext der Dateiübermittlung nur um speicherplatzsparende, komprimierende «Container» mit Dateiformatendungen .zip/.7z. Sie werden nicht für die Langzeitaufbewahrung oder -archivierung verwendet.

Antrag

[1]Die verfahrensleitenden und die verfahrensbeteiligten Behörden erstellen ihre Dokumente zur Übermittlung an die Plattformen im Format PDF/A, die übrigen Verfahrensbeteiligten im Format PDF oder PDF/A.

~~[2]Die Beilagen können in jedem Format übermittelt werden.~~

[3~~2~~]Die verfahrensleitende Behörde muss folgende Formate bearbeiten können:

a. schriftliche Unterlagen:	PDF, PDF/A;
b. Bilddateien:	BMP, GIF, JPEG, PNG;
c. Audiodateien:	MP3, OGG, WAV;
d. Videodateien:	AVI, MOV, MKV, MP4;
e. ~~Archivdateien~~ Container-Formate:	ZIP, 7z.

[4~~3~~] **Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann eine Beilage im Originalformat übermittelt werden.** Wird eine Beilage **nicht im Format PDF** ~~in einem anderen Format~~ eingereicht und kann die verfahrensleitende Behörde die Beilage nicht zweckmässig bearbeiten, so fordert sie die einreichende Person oder Behörde auf, die Beilage in einem von der verfahrensleitenden Behörde festgelegten Format einzureichen oder den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen.

[5~~4~~]Sie räumt ihr eine angemessene Frist ein.

1.4. Zu Art. 5 (Quittungen)

Wenn nicht alle Dokumente eines Dokumenten-Transfers übermittelt werden können, so soll dies gemäss Abs. 2 lit. d lediglich über einen Vermerk auf der Eingangsquittung ersichtlich werden. Aufgrund der zahlreichen Übermittlungen und geplant automatisierten Ablage der Eingangsquittungen besteht das Risiko, dass der Empfänger die Nicht-Übermittlung von Dokumenten übersieht.

Antrag

Der Empfänger ist über ein zusätzlich zur Eingangsquittung generiertes Dokument darauf hinzuweisen, dass und welche Dokumente nicht übermittelt werden konnten.

Gemäss Abs. 3 müssen die Angaben in der Quittung sowohl vom Menschen als auch von Maschinen lesbar sein. Dabei muss nur die vom Menschen lesbare Quittung mit einem geregelten elektronischen Siegel und einem qualifizierten Zeitstempel versehen werden.

Antrag

Jede Quittung muss ein Siegel oder eine elektronische Signatur aufweisen, damit die Integrität beider Quittungen aufgrund derselben Anforderungen an Qualität und Beweisbarkeit sichergestellt ist.

1.5. Zu Art. 6 und Art. 7 (Siegelung)

Im erläuternden Bericht wird beschrieben, dass der Gesetzgeber die Siegelung der Dokumente für die Akteneinsicht nie beabsichtigte. Aus dem Verordnungs-Text kommt aber nicht hervor, dass die Dokumente für eine Akteneinsicht weder gesiegelt noch mit einem Zeitstempel versehen werden müssen. Die Klärung dieses Sachverhalts sollte abschliessend aus der Verordnung hervorgehen.

Antrag

Sofern auf die Siegelung der Dokumente für die Akteneinsicht verzichtet werden kann, so ist in Art. 6 und Art. 7 eine entsprechende Ergänzung sinnvoll: «Dokumente für die Akteneinsicht müssen weder gesiegelt werden noch über einen Zeitstempel verfügen».

1.6. Zu Art. 8 (Authentifizierung der Benutzerinnen und Benutzer)

Die Verordnung lässt offen, wer die Authentifizierung nachweist und mit welchen Mitteln dieser Nachweis erfolgen kann in Fällen, in welchen die Kantone einen anderen Authentifizierungsdienst nutzen.

Antrag

In der Verordnung ist zu klären, wer die Authentifizierung nachweist und mit welchen Mitteln dieser Nachweis erfolgen kann.

1.7. Zu Art. 9 Abs. 2 (Profile)

Wir regen an, für die Behördenprofile die UID zu verwenden, da bei grossen Behörden zusätzliche UID an Unterorganisationen vergeben werden. Ohne die UID wird die Identifizierung der beteiligten Behörde nicht eindeutig möglich sein, da nicht ersichtlich ist, welche Dienststelle oder welches Amt der Verwaltung das Siegel erstellt hat. Es gilt zu verhindern, dass ein Widerspruch zur UID nach Art. 3 Abs. 1 lit. c Ziff. 7 UIDG entsteht.

Antrag

Für Behördenprofile ist die UID zu verwenden.

1.8. Zu Art. 12 Abs. 2 (Maximale Aufbewahrungsfrist für Dokumente und Virenprüfung)

Wir geben zu bedenken, dass die unbegrenzt verlängerbaren Abrufbarkeitsfristen im Fall der Akteneinsicht dazu führen kann, dass der Speicherbedarf der Plattform erheblich grösser ausfällt.

1.9. Zu Art. 13 (Datensicherheit)

Wie unter Art. 2 Abs. 1 ausgeführt, müssen alle Plattformen gemäss Art. 1 dieselben Anforderungen an die Informationssicherheit und den Datenschutz erfüllen. Die Erfüllung dieser Anforderungen ist in Art. 2 Abs. 1 als Voraussetzung zum Erhalt einer Betriebsbewilligung zu definieren.

Antrag

Die Erfüllung der Anforderungen ist in Art. 2 Abs. 1 zu definieren. Art. 13 kann gestrichen werden.

1.10. Zu Art. 14 (Virenprüfung)

Dass nur Dokumente bis zu 64 MB eine Virenprüfung durchlaufen und grössere Dateien für die Virenprüfung in entsprechend kleinere Dateien aufgespalten werden, führt zu den im erläuternden Bericht beschriebenen Risiken. Begründet wird dieser Grenzwert mit der begrenzten Leistungsfähigkeit der zentralen Plattform aufgrund der eingesetzten Software und Speicherkapazität. Damit wird die Verantwortung für die Virenprüfung den Nutzenden übertragen und diese müssen aufgrund der Dateigrösse eines Dokumentes entscheiden, ob / welche Virenprüfungen vor der Öffnung eines Dokuments auf der Plattform zusätzlich durchzuführen sind. Die über die Plattform transferierten Dokumente sind mit dieser Regelung als nicht sicher einzustufen. Auch kann eine Beschränkung der Virenprüfung auf 64 MB dazu führen, dass Absender grössere Dateien komprimieren, was zu unbeabsichtigten Qualitätseinbussen bei Beweisverfahren führen kann. Eine nur eingeschränkte Virenprüfung ist nicht akzeptabel und es ist zwingend erforderlich, dass alle auf der Plattform geöffneten Dokumente die Virenprüfung erfolgreich durchlaufen haben.

Antrag

Art. 14 ist wie folgt zu formulieren:

[1]Die Plattformen ~~müssen bei bis zu 64 Megabyte grossen Dateien~~ führen eine Virenprüfung durch~~führen~~.

[2]~~Dokumente ab 64 Megabyte können sie in 64 Megabyte grosse Dokumente aufteilen und diese einer Virenprüfung unterziehen.~~

[3][2]Die Betreiberin der Plattform kann auf Ersuchen der Benutzerin oder des Benutzers auf die Virenprüfung verzichten.

[4]~~Dokumente, bei denen eine Virenprüfung nach Absatz 2 oder keine Virenprüfung durchgeführt wurde, müssen entsprechend gekennzeichnet werden.~~

[5][3]Ein Dokument, bei dem aufgrund der Virenprüfung ein Virus vermutet wird, darf von der Plattform nicht übermittelt werden. Die Plattform informiert die Absenderin oder den Absender, dass das Dokument nicht übermittelt werden konnte, **zusammen mit der Begründung und einem Link auf das Dokument im Container**.

1.11. Zu 6. Abschnitt: Gebühr für die Nutzung der zentralen Plattform

Das VE-VEKJ geht lediglich auf die Gebühr für den Betrieb und die Weiterentwicklung der zentralen Plattform ein und erwähnt im erläuternden Bericht, aus welchem Grund nicht auf die Aufbaukosten eingegangen wird: «Der Bundesrat geht davon aus, dass der Aufbau der zentralen Plattform bei der abschliessenden Inkraftsetzung abgeschlossen ist - andernfalls kann die abschliessende Inkraftsetzung nicht erfolgen. Aus diesen Gründen geht der VE-VEKJ nicht mehr auf die Aufbaukosten im Sinne von Art. 33 BEKJ ein.»

Antrag

Es ist im erläuternden Bericht festzuhalten, dass unter «Abschluss des Aufbaus der zentralen Plattform» ein Abschluss gemäss HERMES inklusive der erteilten Betriebsbewilligung - und nicht etwa nur die Übergabe des laufenden Projekts an die Körperschaft - verstanden wird. Die abschliessende Inkraftsetzung BEKJ bedingt den umfassenden Abschluss des Projekts «Plattform justitia.swiss», andernfalls steht keine adäquate Plattform zur Erfüllung der gesetzlichen Erfordernisse zur Verfügung.

1.12. Zu Art. 16 (Aufteilung der Gebühr)

Der Bund hat sich gem. Art. 33 BEKJ an den Aufbaukosten der zentralen Plattform in Höhe von 25% beteiligt und will sich zukünftig an den Gebühren mit noch 5% beteiligen. Dies stellt die Kantone vor grosse Herausforderungen, zumal, wie im erläuternden Bericht beschrieben, das Projekt Justitia 4.0 die jährlichen Kosten für den Betrieb und die Weiterentwicklung der zentralen Plattform auf 10 - 12 Mio. Franken einschätzt.

Die Erhebung von Pauschalgebühren begrüssen wir. Bund und Kantone verzichten damit auf die Erhebung von Gebühren basierend auf der durchgeführten Anzahl der Transaktionen. Die vorgeschlagene Reduktion des Bundesanteils sowie die dennoch auf dem Transaktionsvolumen basierende Begründung dieser vorgeschlagenen Reduktion können wir nicht nachvollziehen. Ohne die bisherige Beteiligung des Bundes in derselben Höhe werden die Kantone gezwungen, noch höhere Gebühren auf die Verfahrensbeteiligten abzuwälzen. Dies kann im Sinne der Rechtsgleichheit und des Zugangs zum Recht nicht im Interesse des Bundes liegen.

Antrag

Art. 16 Abs. 1 ist wie folgt anzupassen:

[1]Die Gesamthöhe der Gebühr wird wie folgt auf den Bund und die Kantone, die Mitglied der öffentlich-rechtlichen Körperschaft sind, aufgeteilt:

a. Bundesverwaltung und Bundesanwaltschaft: ~~5~~20 Prozent

b. Eidgenössische Gerichte: 5 Prozent

c. Kantone: ~~90~~ 75 Prozent.

Über das VEKJ ist Rechtssicherheit zu schaffen, dass die Höhe der Gebühren für Kantone nicht an eine Mitgliedschaft zur Körperschaft gebunden wird. Gemäss Art. 6 BEKJ kann die Körperschaft Kantonen, die nicht Partei der Vereinbarung sind, ihre Leistungen gegen kostendeckende Vergütung zur Verfügung stellen. Der Bundesrat versteht «kostendeckend» gemäss Botschaft (BBl 2023, 679) inklusive Investitionskosten. Aus Sicht der Kantone, die nicht Mitglieder der Körper-

schaft sind, ist «kostendeckend» so zu verstehen, dass darüber hinaus kein Gewinn erzielt werden darf.

Antrag

Art. 16 Abs. 2 ist wie folgt zu präzisieren:

[2]Der Anteil der **die Plattform nutzenden** Kantone wird gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung ~~auf die an der Vereinbarung beteiligten Kantone~~ aufgeteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen im Zeitpunkt der Festlegung nach Art. 15.

1.13. Zu Art. 24 (Elektronische Übermittlung unter Behörden)

Im erläuternden Bericht bei der Beschreibung der Zustellungen unter Behörden gem. ZPO wird nicht der korrekte Artikel formuliert. Beschrieben wird der Art. 128**b** Abs. 2 ZPO und nicht wie erwähnt der Art. 128**c** Abs. 2 ZPO.

1.14. Zu 2. Abschnitt: Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Im erläuternden Bericht ist beschrieben, dass erfolgreiche Pilotprojekte mit der zentralen Plattform auch für Schuldbetreibungs- und Konkursverfahren durchgeführt worden sind und dass die Bestimmung zum «eSchKG» aus der VeÜ-ZSSV zukünftig mit dem BEKJ auf Gesetzesstufe gehoben wird (Art. 33b SchKG). Mit der im VE-VEKJ beschriebenen Delegation der entsprechenden Regelungskompetenz an das EJPD kommt nun aber nicht hervor, ob und welche Anpassungen sich bezüglich der Nutzung der Plattform für das Schuldbetreibungs- und Konkursverfahren ergeben. Über Abs. 2 wird lediglich stipuliert, dass die «Betreiberin der Zustellplattform für jede Verbundteilnehmerin ein Postfach einrichten» muss. Im erläuternden Bericht wird dazu lediglich festgehalten, dass der Begriff «Postfächer» nicht im Sinne von E-Mail-Postfächern verstanden wird, sondern die «spezifische eSCHKG-Terminologie mit Postfächern» verwendet wird. Bereits heute bestimmt Art. 14 Abs. 3 VeÜ-ZSSV, dass für jede Verbundteilnehmerin und jeden Verbundteilnehmer auf der Zustellplattform ein Postfach einzurichten ist.

Antrag

Im Sinne der Rechtssicherheit ist im VE-VEKJ klar zu präzisieren, auf welcher Plattform (SEDEX vs. Plattform nach BEKJ) Postfächer zu eröffnen sind.

2. Fremdänderungen

Abschliessend möchten wir die Gelegenheit nicht verpassen, Sie auf eine für uns wichtige Anpassung der StPO hinzuweisen. In Art. 80 und Art. 353 StPO wird konzis definiert, welche Personen bei einem Papierversand die Unterschriften zu leisten haben. Diese starre Unterschriftenregelung ist in der Praxis nur sehr aufwändig umzusetzen und unseres Erachtens nicht notwendig.

Antrag

Die Art. 80 Abs. 2 und Art. 353 Abs. 1 lit. k StPO sind flexibler zu formulieren.

Für Ihre Kenntnisnahme und die wohlwollende Prüfung unserer Anliegen danken wir Ihnen bestens.

IM NAMEN DES REGIERUNGSRATES

Sig.
Susanne Schaffner
Frau Landammann

Sig.
Yves Derendinger
Staatsschreiber

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Justiz-
und Polizeidepartement
Bundeshaus West
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 89 42
info.sk@sg.ch

St.Gallen, 18. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Vernehmlassungsantwort

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 13. März 2026 laden Sie uns zur Vernehmlassung zum Vorentwurf zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VE-VEKJ) ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Die Vorlage, die zum Ziel hat, das Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz (SR 172.023) umzusetzen, erscheint in sich schlüssig und nachvollziehbar und wird deshalb im Grundsatz begrüsst.

Die technischen Anforderungen an die Plattform sind von hohem Interesse für die Kantone, einerseits für die Anbindung ihrer kantonalen Fachanwendungen (insbesondere Geschäftsverwaltungssysteme). Anderseits ergibt sich dieses Interesse daraus, da sich die Plattform justitia.swiss gemäss Information des Bundesamtes für Justiz am Magglinger Rechtsinformatikseminar vom 28. April 2026 voraussichtlich neu auf sämtliche Verwaltungsverfahren auf Bundesebene («admin.swiss») erstrecken und die Plattform zusätzlich den Kantonen für sämtliche (und nicht nur die streitigen) Verwaltungsverfahren zur Verfügung gestellt werden soll. Für die Kantone sind diese Spezifikationen folglich nicht nur aus technischer Sicht von Interesse, sondern auch rechtlich für die entsprechenden Regelungen auf Verordnungsstufe, zumal sie ihre elektronischen Verwaltungsverfahren eigenständig regeln. Im Kanton St.Gallen ist das entsprechende Rechtsetzungsprojekt bereits in parlamentarischer Behandlung.[1] Der Vollzug ist auf den 1. Januar 2027 geplant und das Verordnungsrecht wird zurzeit erarbeitet. Nach Art. 2 Abs. 2 VE-VEKJ regelt das Eidgenössische Justiz- und Polizeidepartement (EJPD) die funktionalen und betrieblichen Anforderungen an die Plattform, insbesondere in Bezug auf die Schnittstellen, in einer Departementsverordnung, die noch erarbeitet wird. Zusätzlich wird geprüft, ob ein Merkblatt mit Bewilligungsvoraussetzungen und Prüfungspunkten erstellt werden soll. In der Folge

[1] X. Nachtrag zum Gesetz über die Verwaltungsrechtspflege und V. Nachtrag zum Planungs- und Baugesetz (22.26.03/22.26/04); abrufbar unter www.ratsinfo.sg.ch/gremium/468/geschaefte/6676.

wäre es für eine möglichst gelingende Harmonisierung für die Kantone von grossem Interesse, wenn ihnen sowohl frühzeitig gewichtige Änderungen am VEKJ-Vorentwurf mitgeteilt würden und sie zur Vernehmlassung zur EJPD-Departementsverordnung begrüsst würden. Ebenso erscheint aus unserer Sicht die Erstellung eines Merkblatts als sehr hilfreich, wobei dies möglichst zeitnah veröffentlicht werden sollte.

In Bezug auf die elektronische Übermittlung unter Behörden (Art. 24 VE-VEKJ) ist darauf hinzuweisen, dass im Kanton St.Gallen im Rahmen des Datenmanagements ein Ansatz verfolgt wird, wonach Verfahrensakten bzw. Verfahrensdokumente grundsätzlich nicht zwischen Behörden übertragen, sondern der Übergang der «Aktenhoheit» über die Vergabe bzw. Anpassung von Zugriffsrechten gesteuert wird. Die Daten sollen bei dieser Konzeption über die gesamte Verfahrenskette hinweg zentral gehalten werden, wobei die jeweils zuständige Behörde den Zugriff auf bzw. die Hoheit über die Dokumente erhält. Das bedeutet, dass sich je nach Stand des Verfahrens die organisatorische Verantwortung («Ownership») einer Datei auf der Ebene der Metainformation ändert, eine Datei jedoch nicht im eigentlichen Sinn übermittelt wird und ihren Speicherort nicht verlässt. Es stellt sich die Frage, ob Art. 24 VE-VEKJ diesen Ansatz ausreichend berücksichtigt bzw. erfasst. Vor diesem Hintergrund erscheint es angezeigt, die Bestimmungen im VE-VEKJ derart zu präzisieren bzw. zu ergänzen, dass auch ein Datenkonzept abgedeckt ist, bei dem der Datenaustausch nicht durch Übermittlung, sondern durch eine kontrollierte Zugriffsgewährung erfolgt.

Die in Art. 2 Abs. 1 Bst. c VE-VEKJ festgehaltene Grössenbeschränkung auf 2 Gigabyte je Dokument erachten wir als deutlich zu tief angesetzt, zumal Dateien regelmässig grösser ausfallen dürften. Weiterer Anpassungsbedarf erscheint u.a. in Bezug auf das Format der Dokumente nach Art. 4 VE-VEKJ angezeigt. Zum einen erscheint die Regelung zur Übermittlung widersprüchlich und könnte zu einem Flickenteppich an technischen Vorgaben führen. Deshalb ist eine Klarstellung mit einem klaren Katalog zu empfehlen, welche Formate durch die öffentlichen Organe zwingend akzeptiert werden. Zum andern erscheint es angezeigt, weitere Formate in die Auflistung in Art. 4 Abs. 3 VE-VEKJ aufzunehmen. Zudem soll die Einhaltung der Formate bereits beim Upload technisch sichergestellt werden, damit kein Effizienzverlust entsteht. Sodann ist darauf hinzuweisen, dass die beschuldigte Person die Mitwirkung im Strafverfahren verweigern kann und deshalb nicht verpflichtet werden kann, eine Beilagen-Datei in einem anderen Format einzureichen. Im Strafverfahren fallen Beweise zudem technisch nicht ausschliesslich in denjenigen Datei-Formaten an, die durch eine Verordnung festgelegt werden können. Anpassungen bzw. Präzisierungen erscheinen ausserdem in Bezug auf die Quittungen nach Art. 5 VE-VEKJ, die Authentifizierung nach Art. 8 VE-VEKJ, die Aufbewahrungsfristen nach Art. 12 VE-VEKJ, die Virenprüfung nach Art. 14 VE-VEKJ, die Digitalisierung von physischen Dokumenten nach Art. 22 VE-VEKJ und den synchronisierten Zeitstempel nach Art. 23 Bst. b VE-VEKJ angezeigt. Ferner besteht Anpassungsbedarf in Bezug auf die Rücksendung von Dokumenten und das Festhalten am eigenhändigen, formerhaltenden Unterschrifterfordernis bei der Zustellung auf Papier.

Bitte entnehmen Sie unsere detaillierten Anmerkungen zu einzelnen Bestimmungen dem Anhang zu diesem Schreiben.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Im Namen der Regierung

Dr. Laura Bucher
Präsidentin

Dr. Benedikt van Spyk
Staatssekretär

Beilage:
Anhang

Zustellung nur per E-Mail (pdf- und Word-Version) an:
cornelia.perler@bj.admin.ch

Anhang zur Vernehmlassungsantwort «Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)»

Die Regierung des Kantons St.Gallen weist im Zusammenhang mit der genannten Vorlage im Einzelnen auf folgende Punkte im Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (nachfolgend VE-VEKJ) hin:

Zu Art. 2 VE-VEKJ *(Anforderungen an die Plattformen):*

Die technischen Anforderungen an die Plattform sind von hohem Interesse für die Kantone, einerseits für die Anbindung ihrer kantonalen Fachanwendungen (insbesondere Geschäftsverwaltungssysteme). Anderseits ergibt sich dieses Interesse daraus, da sich die Plattform justitia.swiss gemäss Information des Bundesamtes für Justiz am Magglinger Rechtsinformatikseminar vom 28. April 2026 voraussichtlich neu auf sämtliche Verwaltungsverfahren auf Bundesebene («admin.swiss») erstrecken und die Plattform zusätzlich den Kantonen für sämtliche (und nicht nur die streitigen) Verwaltungsverfahren zur Verfügung gestellt werden soll. Für die Kantone sind diese Spezifikationen folglich nicht nur aus technischer Sicht von Interesse, sondern auch rechtlich für die entsprechenden Regelungen auf Verordnungsstufe, zumal sie ihre elektronischen Verwaltungsverfahren eigenständig regeln. Im Kanton St.Gallen ist das entsprechende Rechtsetzungsprojekt bereits in parlamentarischer Behandlung.[1] Der Vollzug ist auf den 1. Januar 2027 geplant und das Verordnungsrecht wird zurzeit erarbeitet. Nach Art. 2 Abs. 2 VE-VEKJ regelt das Eidgenössische Justiz- und Polizeidepartement (EJPD) die funktionalen und betrieblichen Anforderungen an die Plattform, insbesondere in Bezug auf die Schnittstellen, in einer Departementsverordnung, die noch erarbeitet wird. Zusätzlich wird geprüft, ob ein Merkblatt mit Bewilligungsvoraussetzungen und Prüfungspunkten erstellt werden soll. In der Folge wäre es für eine möglichst gelingende Harmonisierung für die Kantone von grossem Interesse, wenn ihnen sowohl frühzeitig gewichtige Änderungen am VEKJ-Vorentwurf mitgeteilt würden und sie zur Vernehmlassung zur EJPD-Departementsverordnung begrüsst würden. Ebenso erscheint aus unserer Sicht die Erstellung eines Merkblatts als sehr hilfreich, wobei dies möglichst zeitnah veröffentlicht werden sollte.

Zu Art. 2 Abs. 1 Bst. c VE-VEKJ im Besonderen *(Grössenbeschränkung von 2 Gigabyte je Dokument):*

Die Grössenbeschränkung von 2 Gigabyte (GB) ist deutlich zu tief angesetzt und würde insbesondere Standartübermittlungen der Strafbehörden – und damit den ordentlichen Geschäftsgang der Staatsanwaltschaft – merklich erschweren:

- Mit Einführung des Art. 78a der Schweizerischen Strafprozessordnung (SR 312.0; abgekürzt StPO; vgl. auch Art. 78 Abs. 6bis nStPO, Art. 316 Abs. 3bis nStPO) werden Einvernahmen bei der Staatsanwaltschaft vermehrt auf Video aufgenommen und später gestützt auf die Aufnahme protokolliert. Die Videodateien sind im Regelfall 4 bis 6 GB gross, selten jedoch kleiner. Damit wird die Plattform mit einer Grössenbeschränkung von 2 GB zum ständigen «Stolperstein». Es müssten praktisch alle Videoeinvernahmen in kleinere Dateien aufgeteilt werden.

---

1 X. Nachtrag zum Gesetz über die Verwaltungsrechtspflege und V. Nachtrag zum Planungs- und Baugesetz, 22.26.03/22.26/04, abrufbar unter www.ratsinfo.sg.ch/gremium/468/geschaefte/6676.

- Ebenso verhält es sich bei Dateien, die von sichergestellten Mobiltelefonen mittels forensischen Tools von der Polizei aufbereitet wurden: Die Index-Dateien sind in der Regel mehrere GB gross – je nach Speicherplatz des Mobiltelefons und dessen Nutzung über 100 GB.

- Bei der Aufteilung von Dateien ist zudem zu beachten, dass dies nicht mit «Windows-Bordmitteln» möglich ist. Dazu sind Drittanbieter-Tools wie 7-Zip, WinZip oder WinRar nötig. Das bedeutet wiederum, dass auch die Empfängerinnen und Empfänger der Dateien-Teile die entsprechenden Tools einsetzen müssen, damit sie sie wieder zusammenfügen können.

- Entgegen den Ausführungen im Erläuternden Bericht (S. 6 und 11) sind die Beschränkungen von 2 GB gerade nicht in den allermeisten Fällen ausreichend: Einvernahmen und Befragungen als Videoaufzeichnungen, Mobiltelefonauswertungen sowie Auswertungen von Datenträgern gehören im Vergehens- und Verbrechensbereich zum «Standardrepertoire» der Beweissicherung bzw. Beweisführung. Entsprechende Auswertungen müssen nicht nur von der Polizei an die Staatsanwaltschaft und von dieser an die Gerichte, sondern auch an die berufsmässig handelnden Rechtsvertreterinnen und -vertreter (Art. 103c nStPO) übermittelt werden (Akteneinsicht, Art. 101 StPO). Art. 100 Abs. 3 nStPO bestimmt, dass die Strafbehörden grundsätzlich alle Akten elektronisch führen, nach Art. 102 Abs. 2 Satz 2 nStPO wird Personen, die mit der Strafbehörde elektronisch kommunizieren, die Akteneinsicht auf einer Plattform nach dem BEKJ gewährt. Berufsmässig handelnde Rechtsbeistände müssen den Austausch von Dokumenten mit der Strafbehörde über eine Plattform nach dem BEKJ abwickeln (Art. 103c nStPO). Die im Erläuternden Bericht als Ausnahmefall bezeichnete Dateigrösse von über 2 GB stellt – ausserhalb der Bagatellkriminalität – faktisch den Regelfall dar. Eine Aufteilung grosser Dateien in kleinere (Erläuternder Bericht, S. 6) ist in der Praxis nicht nur aufwendig, sondern auch kaum praktikabel (fehlendes persönliches «Knowhow», personelle Ressourcen, Software, zeitliche Aspekte [u.a. dringliche Haftverfahren], jeweils auf Seiten der Strafbehörden [Polizei, Staatsanwaltschaft, Gerichte] sowie der berufsmässig handelnden Rechtsbeistände [Art. 103c nStPO, Art. 127 ff. StPO]).

- Es ist als praxisfern zu bezeichnen, dass die Betreiberinnen der Plattformen in die Übermittlung grösserer Dokumente einwilligen *können* (Erläuternder Bericht, S. 11) – und nicht müssen. Gerade unter zeitlichem Druck (Haftverfahren oder dringliche gerichtlich-genehmigungspflichtige technische Zwangsmassnahmen usw.) *müssen* auch grosse Dateien *jederzeit* (rund um die Uhr, sieben Tage die Woche) von *sämtlichen Mitarbeitenden* der Strafbehörden, und nicht nur von spezifischen Benutzerinnen und Benutzern, *unkompliziert* und *ohne Bewilligungsauflagen* (u. dgl.) über die Plattform übermittelt werden können. Es kann nicht sein, dass die Strafbehörden hier auf den Goodwill der Plattformbetreiberinnen angewiesen sind und es in deren Belieben steht, Dokumente über 2 GB überhaupt zu übermitteln.

***Zu Art. 4 VE-VEKJ** (Format der Dokumente):*

Der Verordnungsentwurf sieht in Art. 4 Abs. 2 VE-VEKJ vor, dass Beilagen in jedem Format übermittelt werden können. Dies steht u.E. in einem Widerspruch zu Abs. 3, worin konkrete Formate geregelt werden und dadurch direkt Abs. 2 wieder eingeschränkt wird. Im Erläuternden Bericht wird zu Abs. 4 und 5 weiter ausgeführt, dass die Behörden in einem Merkblatt festlegen können, welche Formate von ihnen verwendet werden. Dies führt zu einem Flickenteppich an technischen Vorgaben. So könnte es vorkommen, dass eine Vorinstanz ein Format akzeptiert, das die Rechtsmittelinstanz nicht mehr akzeptiert. Wir empfehlen eine Klarstellung mit einem klaren Katalog, welche Formate durch die öffentlichen Organe zwingend akzeptiert werden. Dieser könnte entweder im Anhang zur Verordnung oder in der EJPD-Departementsverordnung geführt werden.

Zu Art. 4 Abs. 3 VE-VEKJ im Besonderen *(Formate, die von der verfahrensleitenden Behörde bearbeitet werden können muss):*

- Damit kein Effizienzverlust entsteht, muss die Einhaltung der Formate bereits beim Upload technisch sichergestellt werden.

- Die Polizei arbeitet mit iPhones und iPads von Apple. Diese Geräte speichern Fotos standardmässig im HEIC-Format ab. Fotos, die von der Polizei an Tatorten gemacht werden, liegen dann oft in diesem Format vor und werden auch so weitergegeben. Um aufwändige Konvertierungen und nachträgliche Anweisungen an die einreichenden Personen zu vermeiden (Art. 4 Abs. 4 VE-VEKJ), sollte die Plattform das Format ebenfalls unterstützen. Zudem sind Apple iPhones bei der Schweizer Bevölkerung mit einem Marktanteil von 50 % vertreten. Es ist also sehr wahrscheinlich, dass an einem Verfahren beteiligte Personen (ggf. über ihre Rechtsbeistände) Fotos in diesem Format einreichen werden bzw. solche mittels Zwangsmassnahmen (Editionen, Hausdurchsuchungen) behördlich in die Strafverfahren eingeführt werden.

- Weiter ist damit zu rechnen, dass sich Anbieter von Geschäftsverwaltungsprogrammen von Behörden und Anwaltschaft sowie die behördlichen Informatik-Dienste bei der softwaremässigen Ausstattung der Hardware an diesen Formaten als «Mindeststandard» orientieren werden (vgl. Erläuternder Bericht, S. 12 zu Art. 2 Abs. 2 VE-VEKJ). Ein möglichst realitätsbezogenes Abbild der Datei-Formate trägt zu effizienten und ressourcenschonenden Abläufen und Interaktionen seitens Strafbehörden sowie der Anwaltschaft bei.

- Da eine Vielzahl von Softwarelösungen, insbesondere Kommunikationslösungen, «Opus» einsetzen, regen wir an, dieses Format in Bst. c aufzunehmen.

- Aufgrund der verschiedenen verfügbaren Codecs erachten wir die Liste der Videoformate als unzureichend und regen an, die Liste unter Bst. d mit den gängigsten Codecs wie z.B. H.264, H.265, VP9 und AV1 zu ergänzen.

- In Anbetracht von zunehmenden Open-Source-Lösungen, insbesondere basierend auf Linux-Systemen, erachten wir es als angezeigt, das Formal «GZ/TAR GZ» unter Bst. e aufzunehmen.

Zu Art. 4 Abs. 4 und 5 VE-VEKJ im Besonderen *(Aufforderung an einreichende Person oder Behörde, die Beilagen in einem von der Verfahrensleitung festgelegten Format einzureichen oder den Zugriff in geeigneter Weise zu ermöglichen sowie Fristansetzung):*

- Eine beschuldigte Person kann die Mitwirkung im Strafverfahren verweigern (Art. 113 StPO). So kann sie nicht verpflichtet werden, eine Beilagen-Datei in einem anderen Format einzureichen. Gleiches muss auch für die beruflich handelnden Rechtsbeistände (Art. 103c nStPO) gelten, welche *für* die beschuldigten Personen im Rahmen der Mandatsführung entsprechende Eingaben bei den Strafbehörden vornehmen. Dass – wie im Erläuternden Bericht (S. 15, zu Art. 4 Abs. 2 VE-VEKJ) ausgeführt – das Risiko der prozessualen Verwendbarkeit beim Absender liegt und die anwaltlichen Sorgfaltspflichten gegen eine Übermittlung ausserhalb des Katalogs der Datei-Formate (Art. 4 Abs. 3 VE-VEKJ) sprechen, darf bezweifelt werden. Als ultima ratio müssen die Strafbehörden zugehörige EDV-Anlagen/Software mittels Zwangsmassnahmen (Hausdurchsuchung, Beschlagnahme) zur Wahrnehmbarmachung der Dateiinhalte erhältlich machen.

- Gewisse Dateiinhalte sind ausschliesslich mit spezifischen (und «exotischen») Viewern, Playern, Readern usw. wahrnehmbar machbar. Es kann nicht sein, dass ein Gericht die Staatsanwaltschaft auffordert, eine Beilagen-Datei in ein anderes Format zu konvertieren. Die Strafverfolgungsbehörden interagieren mit der «Umwelt», so wie sie sich im Zeitpunkt der Beweiserhebung darstellt. Entsprechend fallen Beweise technisch nicht ausschliesslich in denjenigen Datei-Formaten an, welche durch eine Verordnung festgelegt werden können, sondern so wie sie in der «Umwelt» zu einem bestimmten Zeitpunkt entstehen (z.B. Überwachungsvideo eines Bankinstituts/eines Tankstellenbetreibers/eines Transportunternehmens; elektronische Buchhaltung eines Treuhänders; Plandateien eines Ingenieurs usw.). Die Strafverfolgungsbehörden führen die Beweise in einem «wahrnehmbaren» Zustand ins Verfahren ein, womit es sein Bewenden haben muss, selbst wenn dafür auf spezifische Softwareapplikationen zurückgegriffen werden muss. Ist ein Beweis technisch nicht wahrnehmbar zu machen, erfüllt er die Beweiszwecke nicht; diese «Wahrnehmbarmachung» darf jedoch nicht durch einen abschliessenden Format-Katalog eingeschränkt werden. Auch ist darauf hinzuweisen, dass bei einer Konvertierung von Dateien (z.B. in das PDF-Format) «verborgene» Informationen – welche für die Beweisführung notwendig sind – «verloren» gehen können (z.B. Metadaten wie Benutzerinformationen sowie Erstellungs- und Zugriffszeitpunkte).

- In Bezug auf die Frist nach Abs. 5 erachten wir es als sinnvoll, einen konkreten Zeitrahmen festzulegen.

Zu Art. 5 Abs. 2 Bst. g VE-VEKJ *(Quittungen):*

Wenn in der Quittung nur der Name der vertretenen Person erscheint, nicht aber derjenige der handelnden Person, ist im Nachhinein nicht mehr feststellbar, wer die Handlung tatsächlich vorgenommen hat. Dies ist insbesondere bei fehlerhaften Eingaben oder dem Entzug der Vertretungsbefugnis essenziell. Wir regen an, auch den Namen der handelnden Person zu führen.

Zu Art. 5 Abs. 4 VE-VEKJ *(Format der Quittungen):*

Im Sinn einer Standardisierung erachtet wir es als notwendig, dass das Format für maschinenlesbare Quittungen mindestens eingegrenzt, vorzugsweise definiert wird. Dies ist insbesondere im Zusammenhang mit Art. 5 Abs. 5 VE-VEKJ nötig, der für die von Maschinen lesbare Form ein geregeltes elektronisches Siegel und einen qualifizierten elektronischen Zeitstempel nicht als zwingend voraussetzt. Darin besteht das Risiko inkonsistenter Informationen zwischen den von Menschen und von Maschinen lesbaren Quittungen. Ohne Formatvorgaben wird dies noch begünstigt.

Zu Art. 8 Abs. 3 VE-VEKJ *(andere Authentifizierungsdienste):*

Wir erachten es als notwendig, zu präzisieren, was als «angemessenes Schutzniveau» gilt.

Zu Art. 12 VE-VEKJ *(Aufbewahrungsfristen):*

Art. 12 Abs. 1 VE-VEKJ sieht vor, dass auf einer Plattform gespeicherte Dokumente und Quittungen sechs Monate nach der Entgegennahme bzw. nach der Erstellung automatisch vernichtet werden. Diese Regelung könnte dazu führen, dass zentrale Dokumente noch während eines laufenden Verfahrens von der Plattform entfernt werden. Es ist dabei sicherzustellen, dass die betroffenen Personen und Organe auf die Löschung hingewiesen werden, sodass sie die Dokumente in ihre persönliche Ablage überführen können. Denkbar wäre zudem, dass zumindest für

die Quittungen eine längere Aufbewahrungsfrist vorgesehen wird (z.B. drei Jahre wie im Rahmen von Nachforschungen bei der Schweizerischen Post im Briefverkehr).

***Zu Art. 14 VE-VEKJ** (Virenprüfung):*

- Art. 14 VE-VEKJ sieht eine notwendige Virenprüfung bei Dokumenten vor (ausgenommen sind PDF und PDF/A Formate). Dabei äussert sich der Erläuternde Bericht nicht, ob und wie die bei der Virenprüfung verarbeiteten Daten protokolliert, gespeichert oder gelöscht werden. Dies sollte ergänzt werden.

- Der Begriff «Dokumente» in diesem Artikel schliesst alle anderen Arten von Daten aus. Dies erachten wir in Anbetracht der zugelassenen Formate nach Art. 4 Abs. 3 VE-VEKJ als nicht zweckmässig.

- Die Beschränkung auf 64 MB im Vergleich zur maximal zulässigen Dateigrösse je Datei nach Art. 2 Abs. 1 Bst. c VE-VEKJ erscheint nicht zielführend. Es gibt keine technische Begründung für die Limitierung. Die Virenprüfung muss sich an der besagten maximal zulässigen Dateigrösse ausrichten. Mit Blick auf die maximal zulässige Dateigrösse erschliesst sich zudem die Notwendigkeit von Art. 14 Abs. 2 VE-VEKJ nicht.

***Zu Art. 22 Abs. 3 und 4 VE-VEKJ**; vgl. auch Art. 29 BEKJ (Digitalisierung von physischen Dokumenten; OCR-Erkennung und inhaltliche Übereinstimmung – Verpflichtung zur Qualitätskontrolle):*

- Bei der Digitalisierung von physischen Dokumenten wird ein Abbild (Foto) des Originals erstellt und der darauf enthaltene Bild-Text in bearbeitbaren Text umgewandelt. Dabei können Buchstaben falsch erkannt werden (z.B. I als 1, B als 8, rn als m usw.). Daher wird immer eine Diskrepanz zwischen dem Text des physischen Originals und dem digitalisierten, interpretierten bzw. erkannten Text bestehen. Aus diesem Grund stimmt der Inhalt eines physischen Dokuments nie wirklich mit dem Text des digitalisierten Dokumentes überein. Entsprechend kann eine «inhaltliche» Übereinstimmung mittels OCR nicht gewährleistet werden; eine «händische» bzw. «optische» nachträgliche Qualitätskontrolle digitalisierter – sprich mit OCR gescannter Textdateien – ist aufwandmässig nicht möglich.

- Nach Art. 29 Abs. 1 BEKJ lesen die Behörden physisch eingereichte Dokumente elektronisch ein, ausgenommen sind Dokumente, die sich aus technischen Gründen nicht dafür eignen. Auf der einen Seite geht aus dem Wortlaut des Gesetzes nicht hervor, wie mittels Zwangsmassnahmen erhältlich gemachten physischen Dokumenten zu verfahren ist (diese wurden nicht «eingereicht»; sinnvollerweise werden solche jedoch auch digitalisiert). Auf der anderen Seite ist eine Qualitätskontrolle, so wie im Erläuternden Bericht (S. 32 zu Art. 22 Abs. 3 VE-VEJK) ausgeführt, bei umfangreichen physischen Sicherstellungen/Beschlagnahmungen (tausende Seiten von Papier bei Wirtschaftsdelikten) nicht möglich. Es muss mit einer stichprobenartigen manuellen Überprüfung sein Bewenden haben.

- Sodann wäre in Art. 22 Abs. 4 VE-VEKJ zu ergänzen, dass mit «bildlich» der «Image-Layer» und mit «inhaltlich» der «Text-Layer (maschinenlesbarer Text)» gemeint ist. Diese Präzisierung soll OCR-Artefakten vorbeugen, respektive inkonsistente Informationen verhindern.

Zu Art. 23 Bst. b VE-VEKJ *(synchronisierter Zeitstempel):*

Es erscheint angezeigt, systemseitig einen Standard für die Synchronisierung der Zeitstempel zu verlangen, z.B. UTC + Offset gem. Standard ISO 8601-2-2019/AMD 1:2025.

Zu Art. 24 VE-VEKJ *(elektronische Übermittlung unter Behörden):*

Diese Bestimmung geht bei der elektronischen Übermittlung von Dokumenten zwischen Behörden konzeptionell von einer Übertragung von Daten aus. Demgegenüber wird im Kanton St.Gallen im Rahmen des Datenmanagements ein Ansatz verfolgt, wonach Verfahrensakten bzw. Verfahrensdokumente grundsätzlich nicht zwischen Behörden übertragen, sondern der Übergang der «Aktenhoheit» über die Vergabe bzw. Anpassung von Zugriffsrechten gesteuert wird. Die Daten sollen bei dieser Konzeption über die gesamte Verfahrenskette hinweg zentral gehalten werden, wobei die jeweils zuständige Behörde den Zugriff auf bzw. die Hoheit über die Dokumente erhält. Das bedeutet, dass sich je nach Stand des Verfahrens die organisatorische Verantwortung («Ownership») einer Datei auf der Ebene der Metainformation ändert, eine Datei jedoch nicht im eigentlichen Sinn übermittelt wird und ihren Speicherort nicht verlässt. Zu diesem Zweck wird im Kanton St.Gallen mit dem Projekt «NeDaV» als Teil des Programms «Ablösung Juris-4» eine zentrale Plattform für Daten geschaffen.

Mit Blick auf die Konzeption des Datenmanagements stellt sich die Frage, ob Art. 24 VE-VEKJ diesen Ansatz ausreichend berücksichtigt bzw. erfasst. Zwar lässt Abs. 1 «andere technisch geeignete Lösungen» zu, spricht aber gleichwohl von einer Übermittlung von Dokumenten. Abs. 2 knüpft ausdrücklich an den Zeitpunkt der Übermittlung sowie an übermittelte Dokumente an. Dies könnte so verstanden werden, dass Lösungen ohne eigentliche Datenübertragung nicht erfasst sind oder zumindest für solche Datenmanagementlösungen rechtlich eine Lücke bestehen könnte.

Der im Kanton St.Gallen verfolgte Ansatz bietet insbesondere hinsichtlich Effizienz, Datenkonsistenz und Nachvollziehbarkeit Vorteile, da Mehrfachspeicherungen und Übertragungsprozesse entfallen. Art. 24 Abs. 2 VE-VEKJ entsprechend werden der Zeitpunkt der Übergabe, die Namen der übergebenen Daten, deren jeweilige Grösse und Hashwert gespeichert. Vor diesem Hintergrund erscheint es angezeigt, die Bestimmungen im VE-VEKJ derart zu präzisieren bzw. zu ergänzen, dass auch ein Datenkonzept abgedeckt ist, bei dem der Datenaustausch nicht durch Übermittlung, sondern durch eine kontrollierte Zugriffsgewährung erfolgt.

Eine mögliche Anpassung von Art. 24 VE-VEKJ könnte wie folgt aussehen:

Art. 24 VE-VEKJ Elektronische Übermittlung unter Behörden

[1] Abweichend von Artikel 128*c* Absatz 1 ZPO, Artikel 103*c* Absatz 1 StPO und Artikel 8*d* Absatz 1 OHG können die Behörden untereinander andere technisch geeignete Lösungen zur elektronischen Übermittlung von Dokumenten **oder zur Gewährung des elektronischen Zugriffs auf Dokumente** verwenden.

[2] Sie müssen gewährleisten, dass **die für den elektronischen Austausch massgeblichen Vorgänge, insbesondere** der Zeitpunkt der Übermittlung **oder der Zugriffsgewährung sowie des Zugriffs**, der Dokumente, die Namen, die Grösse und die Hashwerte aufgezeichnet werden und unveränderbar sind.

Mit den vorgeschlagenen Ergänzungen würde klargestellt, dass neben der herkömmlichen Datenübermittlung auch Systeme zulässig sind, bei denen der «Austausch» von Dokumenten durch die Gewährung von Zugriffsrechten erfolgt. Gleichzeitig würde sichergestellt, dass die Anforderungen an die Nachvollziehbarkeit und Integrität der Daten auch für solche Lösungen gelten.

Zu Rücksendung von Dokumenten *(Erläuternder Bericht, Ziff. 2.6, S. 7; Art. 30 BEKJ):*

- Es ist darauf hinzuwirken, dass Art. 30 BEKJ revidiert wird. Eine Rücksendung physisch eingereichter Dokumente nach der (verbindlichen) Digitalisierung verursacht nicht nur hohe Portokosten für den Staat und beansprucht Personalressourcen, sondern ist zudem missverständlich für die Einreichende oder den Einreichenden (z.B. die behördliche Rücksendung einer Strafanzeige spricht für ein Nichteintreten auf die Eingabe; es ist mit telefonischen Rückfragen bei der Staatsanwaltschaft zu rechnen, was wieder personelle Ressourcen bindet). Es muss deshalb den Strafbehörden erlaubt sein, entsprechende Dokumente ohne Rücksendung zu vernichten (sofern die Originaldokumente nicht für die Strafverfahren notwendig sind oder Wertpapiere darstellen). Auch bei behördlichen Aktenbeizügen oder Auskünften (z.B. bei kantonalen und kommunalen Verwaltungsbehörden, die nicht dem Obligatorium der elektronischen Kommunikation unterstehen) ist auf eine Rücksendung der Dokumente nach dem Trägerwandel zu verzichten (sofern es sich nicht um Original-Verfahrensakten handelt).

- Ein physisches Begleitschreiben zur Rücksendung der Dokumente muss im Rahmen der Aktenführungspflicht zusätzlich als Kopie (ggf. zusammen mit der postalischen Aufgabebestätigung) digitalisiert werden (Trägerwandel) und anschliessend zu den elektronischen Verfahrensakten hinzugefügt werden. Dies stellt faktisch einen weiteren, zusätzlichen Arbeitsschritt dar.

Zu Versand in Papierform *(Erläuternder Bericht, Ziff. 2.6, S. 7 f.):*

- Es ist darauf hinzuwirken, dass – zumindest im Bereich von bundesrechtlichen sowie kantonalen Übertretungstatbeständen (inkl. Art. 258 ZPO) – beim Versand von verfahrensabschliessenden Entscheiden (z.B. Strafbefehle) *an Personen, welche nicht elektronisch mit den Strafbehörden kommunizieren*, auf das *eigenhändige, formerhaltende Unterschrifterfordernis verzichtet* wird («Dokument ohne Unterschrift»), dies durch Änderungen von BEKJ und StPO (Art. 353 Abs. 1 Bst. k StPO, Art. 353 Abs. 1 Bst. k nStPO, Art. 80 Abs. 2 nStPO [Art. 201 Abs. 2 Bst. h nStPO] usw.).

- Der «Mehrwert» einer eigenhändigen (formerhaltenden) Unterschrift der ausstellenden Person ist für die Empfängerin bzw. den Empfänger z.B. eines Strafbefehls betreffend eine Strassenverkehrsübertretung nicht ersichtlich. Authentizität und Integrität einer verfahrensabschliessenden Verfügung werden – im Gegensatz zum fristauslösenden Zugangszeitpunkt des Entscheids bei der Empfängerin oder beim Empfänger – kaum bestritten. Ein Missbrauchspotenzial erscheint als äusserst gering.

- Es ist davon auszugehen, dass die überwiegende Mehrheit von (privaten) Personen *nicht* elektronisch mit den Strafbehörden (bzw. Übertretungsstrafbehörden) kommunizieren wird. Gerade im Bereich der Bagatellkriminalität und der dort anfallenden grossen Anzahl an verfahrensabschliessenden Entscheiden (insb. Strassenverkehrsübertretungen) *verhindert die Beibehaltung der (formerhaltenden) eigenhändigen Unterschrift eine ressourcenschonende und effiziente Abarbeitung entsprechender Strafverfahren*. Insbesondere verhindert das

eigenhändige Unterschrifterfordernis einen ausgelagerten, effizienten «Massenversand» von Verfügungen über ein Verarbeitungszentrum (elektronische Übermittlung aus dem Geschäftsverwaltungsprogramm der Strafverfolgungsbehörden oder Übertretungsstrafbehörden an ein Verarbeitungszentrum als PDF [Dokument ohne Unterschrift der ausstellenden Person bzw. faksimilierte Unterschrift der ausstellenden Person], dortiger Ausdruck auf Papier, dortige Verpackung und dortige Frankierung und Übergabe an die Post zum Versand). Das eigenhändige Unterzeichnen von tausenden Verfügungen je Mitarbeiterin bzw. Mitarbeiter (inkl. Ausdruck, Verpackung usw.) stellt für diese bzw. diesen eine nicht zu unterschätzende Arbeitsbelastung dar.

- Eine eigenhändig unterzeichnete Ausfertigung eines Entscheides auf Papier (ebenso eine Vorladung auf Papier) muss im Rahmen der Aktenführungspflicht zusätzlich als Kopie (zusammen mit der postalischen Aufgabebestätigung) digitalisiert werden (Trägerwandel) und anschliessend den elektronischen Verfahrensakten hinzugefügt werden. Dies stellt faktisch einen zusätzlichen Arbeitsschritt dar.

- Die Implementierung von Robotik und Künstlicher Intelligenz betreffend Ausfertigung von Entscheiden im «Massengeschäft» stehen einer eigenhändigen Unterschrift entgegen und widersprechen politischen Forderungen, von der Digitalisierung zwecks Effizienzsteigerung Gebrauch zu machen. Die Digitalisierung und digitale Transformation in der Strafjustiz wird mit dem Festhalten am handschriftlichen Unterschrifterfordernis in nicht mehr vertretbarem Mass behindert. Gleiches gilt zunehmend auch ausserhalb des Bereichs der Entscheidausfertigung bzw. umfasst alles, was noch auf Papier ausgedruckt, handschriftlich unterzeichnet, verpackt, frankiert und versandt werden muss. Im Erläuternden Bericht steht unter Ziff. 6.3 (Auswirkungen auf die Volkswirtschaft, S. 38): «Die Digitalisierung schreitet voran. [...] Wie der Bundesrat bereits bei der Schaffung der ZPO ausgeführt hat, trägt eine effiziente Rechtspflege zur wirtschaftlichen Prosperität und damit letztlich auch zur Lebensqualität bei.» Dem ist Rechnung zu tragen, indem unnötige Formerfordernisse im analogen Raum wenn immer möglich beseitigt werden, damit die Vorteile der Digitalisierung genutzt werden können.

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungskanzlei, 8510 Frauenfeld

Eidgenössisches
Justiz- und Polizeidepartement (EJPD)
Herr Beat Jans
Bundesrat
Bundeshaus West
3003 Bern

Frauenfeld, 16. Juni 2026
Nr. 354

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Vernehmlassung

Sehr geehrter Herr Bundesrat

Wir danken Ihnen für die Möglichkeit der Stellungnahme zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ). Der Regierungsrat anerkennt das Anliegen der Vorlage, sieht jedoch in wesentlichen Punkten Anpassungsbedarf. In der vorliegenden Form stimmt er der Verordnung daher nicht vorbehaltlos zu und bringt die nachfolgenden Einwände vor.

1. Allgemeine Bemerkungen

1.1. Mangelnde Klarheit des Behördenbegriffs (Art. 4, 6 und 24 VE-VEKJ)

Die mangelnde Klarheit des Behördenbegriffs im Vorentwurf schafft erhebliche Rechtsunsicherheit hinsichtlich des persönlichen Geltungsbereichs. Es bleibt offen, welche Stellen als „Behörden" einzustufen sind. Dies betrifft insbesondere öffentlich-rechtliche Anstalten und Organisationen, die regelmässig im Auftrag der Justiz tätig sind, wie Institute für Rechtsmedizin (IRM), forensische Institute, psychiatrische Kliniken oder auch Betriebe des öffentlichen Verkehrs. Da an den Status als Behörde weitreichende Konsequenzen geknüpft sind, insbesondere das Anbindungsobligatorium an die Plattform, die elektronische Aktenführung und die Siegelungspflicht, ist eine präzise Abgrenzung des Geltungsbereichs bereits auf Verordnungsstufe unerlässlich.

Regierungsgebäude, 8510 Frauenfeld
T +41 58 345 53 10
www.tg.ch

1.2. Differenzierung zwischen verfahrensleitenden und verfahrensbeteiligten Behörden

Um eine unverhältnismässige administrative Belastung zu vermeiden, drängt sich eine funktionale Unterscheidung zwischen verfahrensleitenden und lediglich verfahrensbeteiligten Behörden oder „Amtsstellen" auf:

- Einschränkung der Siegelungspflicht: Die Pflicht zur Siegelung gemäss Art. 22 Abs. 2 BEKJ sollte in der VEKJ dahingehend ausgelegt werden, dass sie nur verfahrensleitende Behörden trifft. Diese treten autoritativ auf und begründen durch Verfügungen oder Entscheide Rechte und Pflichten. Daher muss die Authentizität ihrer Dokumente unabhängig von der Plattform jederzeit prüfbar sein.
- Administrative Entlastung verfahrensbeteiligter Stellen: Verfahrensbeteiligte Behörden liefern oft lediglich Registerauszüge oder Akten aus abgeschlossenen Verfahren. Eine flächendeckende Siegelungspflicht für alle Schweizer Behörden auf allen Stufen wäre mit einem enormen organisatorischen Aufwand und beträchtlichen Kosten verbunden, wofür das BEKJ keine hinreichende Grundlage bietet. Die Identifikation dieser Stellen erfolgt bereits hinreichend durch die Authentifizierung auf der Plattform.

1.3. Einsatz der qualifizierten elektronischen Signatur (QES)

Es muss sichergestellt werden, dass die qualifizierte elektronische Signatur (QES) überall dort zum Einsatz kommt, wo das Gesetz die Identifikation der natürlichen Person der Autorenschaft vorschreibt. Dies gilt insbesondere für Sachverständigengutachten (z.B. gemäss Art. 187 StPO), bei denen die forensische Nachverfolgbarkeit der sachverständigen Person prozessrechtlich entscheidend ist. Ein einfaches Behördensiegel ist hierfür nicht ausreichend, da es nur die Institution, nicht aber den konkreten Verfasser beglaubigt.

1.4. Klärung der Rolle der Kantonspolizei

Besondere Aufmerksamkeit ist der Kantonspolizei zu widmen. Aufgrund ihrer engen Zusammenarbeit mit der Staatsanwaltschaft nimmt sie eine zentrale Rolle in der Justizkette ein, agiert jedoch selbst nur in seltenen Fällen als verfahrensleitende Behörde. Zudem hält der erläuternde Bericht in Kapitel 6.2 fest, dass Polizeien ab Inkrafttreten der VEKJ über ein Konto auf der zentralen Plattform verfügen müssen. Damit ist die Kantonspolizei als Nutzerin der Plattform direkt betroffen, ohne dass der Vorentwurf den Geltungsbereich für Polizeibehörden hinreichend regelt. Welche Kommunikationsvorgänge und Geschäfte künftig zwingend über die zentrale Plattform abzuwickeln sind, lässt der Vorentwurf offen.

1.5. Verlagerung technischer Spezifikationen in einen Anhang oder eine Departementsverordnung (Art. 2 und Art. 4 VE-VEKJ)

Die Entwicklungsgeschwindigkeit im IT-Bereich steht in keinem Verhältnis zur Dauer von Rechtsetzungsverfahren. Durch die Festschreibung technischer Standards im Verordnungstext wird riskiert, dass diese bereits bei Inkrafttreten überholt sind. Die Regelung in einem Anhang zur VEKJ oder einer Departementsverordnung erlaubt eine wesentlich flexiblere Anpassung an den technischen Fortschritt, ohne dass jedes Mal eine formelle Revision der gesamten Verordnung notwendig wird. Wir beantragen deshalb, die im Vorentwurf enthaltenen technischen Anforderungen – insbesondere die maximale Dateigrösse (Art. 2 Abs. 1 lit. c), den Katalog der bearbeitbaren Dateiformate (Art. 4 Abs. 3) sowie die Spezifikationen zur Virenprüfung (Art. 14) und zur Digitalisierungsqualität (Art. 22) – aus dem Haupttext der Verordnung zu entfernen.

2. Bemerkungen zu einzelnen Artikeln

Art. 2 Abs. 1 lit. c VEKJ

Die Festlegung funktionaler und betrieblicher Anforderungen an die Plattform sollte nicht auf Verordnungsstufe erfolgen. Stattdessen ist die Kompetenz zur Regelung dieser Anforderungen dem EJPD zu übertragen, damit technische und betriebliche Vorgaben flexibel an neue Entwicklungen angepasst werden können. Insbesondere wird die in Art. 2 Abs. 1 lit. c vorgesehene Obergrenze von 2 Gigabytes für die Grösse elektronischer Sendungen als zu starr erachtet. Solche Limiten sind von technischen Rahmenbedingungen abhängig und können sich aufgrund des technologischen Fortschritts verändern. Anstelle einer festen Grössenbeschränkung in der Verordnung sollte auf die jeweils geltenden technischen Standards oder auf die durch das EJPD festgelegten technischen Vorgaben verwiesen werden. In der Praxis müssten allenfalls auch grössere Dateien wie Videos als Beweismittel übermittelt werden können.

Art. 3 VEKJ

Die Verordnung regelt nicht, ob eine erteilte Bewilligung zeitlich befristet ist oder ob sie unbefristet gilt. Ebenso bleibt offen, ob und in welchen Abständen eine Re-Zertifizierung beziehungsweise eine erneute Überprüfung der Voraussetzungen erforderlich ist. Aus Gründen der Rechtssicherheit und der einheitlichen Anwendung der Verordnung sollte ausdrücklich festgelegt werden, welche Gültigkeitsdauer eine Bewilligung hat und unter welchen Voraussetzungen eine Re-Zertifizierung oder periodische Überprüfung zu erfolgen hat.

Art. 4 VEKJ

Die in der Verordnung vorgesehenen Dateiformate sollten nicht abschliessend auf Verordnungsstufe festgelegt werden. Aufgrund des technologischen Fortschritts ist davon auszugehen, dass künftig neue oder weiterentwickelte Formate zur Verfügung stehen werden. Eine regelmässige Anpassung der Verordnung an technische Entwicklungen wäre wenig praktikabel und würde den notwendigen Handlungsspielraum unnötig einschränken.

Stattdessen sollte auf anerkannte technische Standards oder auf die durch das EJPD festgelegten technischen Vorgaben verwiesen werden. In diesem Zusammenhang ist zu prüfen, ob die Kompetenz zur Definition und Anpassung der zulässigen Dateiformate dem EJPD übertragen werden sollte. Weiter regelt die Verordnung lediglich den Fall, dass eine Behörde eingereichte Beilagen aufgrund eines nicht unterstützten Formats nicht öffnen kann. Nicht geregelt ist hingegen die umgekehrte Situation, in der eine Verfahrenspartei die von einer Gegenpartei eingereichten Dokumente nicht öffnen kann. Für die Praxis ist daher unklar, wer die Verantwortung dafür trägt, dass übermittelte Dokumente von allen Verfahrensbeteiligten geöffnet und gelesen werden können. Die Verordnung sollte diese Frage ausdrücklich regeln und die entsprechenden Verantwortlichkeiten klar festlegen. Wir begrüssen ausdrücklich die derzeit liberale Regelung für Beilagen im Vorentwurf. Insbesondere soll auf die Einführung eines Primats von PDF-Dateien verzichtet werden. Wir lehnen Bestrebungen ab, die auf eine generelle Umwandlung von Justizakten in PDF-Dokumente abzielen. Die Digitalisierung der Justiz darf nicht dazu führen, dass Informationen durch Formatkonversionen entwertet werden. Die Umwandlung von Dokumenten in das PDF-Format führt unweigerlich zur Zerstörung strukturierter Daten und zum Verlust wertvoller Metadaten. Für eine moderne, effiziente Fallbearbeitung ist es jedoch unerlässlich, dass die Justizbehörden mit Originaldaten (Primärdaten) arbeiten können. Nur so lassen sich beispielsweise komplexe Tabellenkalkulationen, Datenbankauszüge oder forensische Datensätze in ihrer vollen Tiefe analysieren und nachvollziehen.

Art. 5 VEKJ

Dieser Artikel ist zu streichen. Dokumente, die den Server der Behörde erreicht haben, müssen als fristgerecht eingereicht gelten, auch wenn sie von der Virenprüfung zurückgewiesen werden. In solchen Fällen ist den Parteien eine Frist zur erneuten Einreichung einzuräumen. Die Regelung im Entwurf gefährdet die Rechtssicherheit und ist anzupassen.

Art. 6 VEKJ

Unter Verweis auf die obigen Ausführungen zum Behördenbegriff wird beantragt, dass die Siegelungspflicht nur die verfahrensleitenden Behörden treffen kann und dass eine

Klärung der Erforderlichkeit der qualifizierten elektronischen Unterschrift aller anderen Verfahrensbeteiligten gewünscht wird, namentlich dort, wo das Gesetz eine Unterschrift der Autorenschaft tragen muss (z.B. sachverständige Personen).

4. Abschnitt: Authentifizierung, Profile, Schnittstellen und Berechtigungen

Die Regelungen zur Authentifizierung sollten um Anforderungen an die Nachvollziehbarkeit der Berechtigungsverwaltung ergänzt werden. Die Plattform sollte die Erteilung, Änderung und den Entzug von Berechtigungen sowie deren Nutzung durch die jeweiligen Benutzerprofile lückenlos protokollieren und nachvollziehbar dokumentieren. Zudem sollte sichergestellt werden, dass die für ein Benutzerprofil geltenden Berechtigungen jederzeit überprüft und nachvollzogen werden können. Dies dient der Transparenz, der Informationssicherheit sowie der Nachweisbarkeit im Rahmen von Audits, Kontrollen oder der Untersuchung von Sicherheitsvorfällen. Eine entsprechende Regelung würde die Governance der Plattform stärken und zu einer rechts- und revisionssicheren Berechtigungsverwaltung beitragen.

Art. 11 VEKJ

Es stellt sich die Frage, ob die in Art. 11 vorgesehenen Überprüfungs- und Aktualisierungspflichten ausschliesslich für Benutzerinnen und Benutzer oder auch für Behörden und Organisationseinheiten gelten sollen. Aus praktischer Sicht wäre es zu begrüssen, wenn auch bei Behörden regelmässig überprüft würde, ob die erteilten Berechtigungen weiterhin erforderlich und gültig sind. Die jährliche Bestätigung der eigenen Berechtigung ist jedoch zu kurz. Dies führt zu unnötigem Aufwand für alle Beteiligten. Die Berechtigung sollte mehrere Jahre gültig sein.

Art. 12 VEKJ

Die Verordnung sieht vor, dass Quittungen sechs Monate nach ihrer Entgegennahme automatisch vernichtet werden. Angesichts der teilweise langen Verfahrensdauern sowie der Möglichkeit, dass eine Quittung auch nach Ablauf von sechs Monaten noch von Bedeutung sein kann und gegebenenfalls noch nicht in ein Geschäftsverwaltungssystem überführt wurde, erscheint diese Frist zu kurz bemessen. In Anlehnung an die Zeitspanne von drei Jahren, innerhalb derer bei der Schweizerischen Post Nachforschungen zu Briefsendungen möglich sind, wird vorgeschlagen, die Aufbewahrungsdauer für Quittungen auf mindestens drei Jahre zu verlängern. Dadurch wird sichergestellt, dass auch bei langdauernden Verfahren oder bei später auftretenden Unklarheiten die notwendigen Nachweise über die elektronische Übermittlung weiterhin zur Verfügung stehen. Es fehlt zudem eine Regelung, die den Beteiligten den Download der Akten und Dokumente in einem gängigen Format (insbesondere PDF) ermöglicht. Die Akteneinsicht sollte nicht ausschliesslich über die browserbasierte Plattform erfolgen. Ergänzend ist vorzusehen, dass die Beteiligten die Akten lokal speichern und archivieren können.

Art. 14 Abs. 1 VEKJ

Die vorgesehene Beschränkung der Virenprüfung auf Dokumente bis zu einer Grösse von 64 Megabyte erscheint als nicht zeitgemäss. Die Grösse eines Dokuments steht in keinem direkten Zusammenhang mit dem Risiko einer Schadsoftware-Infektion. Gerade auch grössere Dateien können Schadsoftware enthalten und ein entsprechendes Sicherheitsrisiko darstellen.

Aus Sicht der Praxis sollten Virenprüfungen deshalb unabhängig von der Dateigrösse grundsätzlich für sämtliche über die Plattform übermittelten Dokumente durchgeführt werden. Auf eine feste Grössenlimite in der Verordnung ist zu verzichten, stattdessen sollte sie den technischen Möglichkeiten der Plattformbetreiber angepasst werden. Die Bestimmung sollte daher so formuliert werden, dass eine angemessene Sicherheitsprüfung aller übermittelten Dokumente sichergestellt wird, ohne diese auf Dateien bis zu einer bestimmten Grösse zu beschränken. Zudem sollte diese Grösse, um mit dem technischen Fortschritt Schritt halten zu können, nicht in der Verordnung, sondern in einem Anhang oder einer Departementsverordnung festgehalten werden.

Art 14 Abs. 5 VEKJ

Es wird begrüsst, dass die Plattform die Behörde darüber informiert, wenn einzelne Dokumente aufgrund technischer Einschränkungen nicht übermittelt werden konnten. Die entsprechende Information sollte jedoch nicht lediglich als Hinweis in der Eingangsquittung enthalten sein. Vielmehr ist sicherzustellen, dass die betroffene Behörde über nicht übermittelte Dokumente ausdrücklich und in geeigneter Weise informiert wird, beispielsweise mittels einer separaten Mitteilung oder eines eigenständigen Dokuments. Andernfalls müssten die verfahrensleitenden Behörden sämtliche Eingangsquittungen systematisch auf entsprechende Hinweise überprüfen, was im praktischen Betrieb mit erheblichem Mehraufwand verbunden und wenig zweckmässig wäre. Die Verordnung beziehungsweise die technischen Vorgaben sollten daher vorsehen, dass Hinweise auf unvollständige Übermittlungen für die empfangende Behörde klar erkennbar und gesondert ausgewiesen werden.

Art. 21 VEKJ

Die vorgesehene periodische Überprüfung der Gebührenregelung wird ausdrücklich begrüsst. Dies gilt insbesondere auch für die regelmässige Überprüfung der Kosten- und Gebührenaufteilung zwischen Bund und Kantonen. Es ist jedoch nicht sicher, ab wann genau mit der regelmässigen Überprüfung begonnen wird. Unter Umständen ist dies erst sieben Jahre nach Inkrafttreten des BEKJ der Fall, da dieses zunächst während fünf Jahren in allen Kantonen umgesetzt werden muss und die zweijährige Frist erst anschliessend zu laufen beginnt.

2. Kapitel: Digitalisierung von physischen Dokumenten

Problematik der Rücksendungspflicht physischer Dokumente (Art. 30 BEKJ):

Die im erläuternden Bericht festgehaltene Auffassung, wonach für eine reduzierende Auslegung von Art. 30 BEKJ kein Handlungsspielraum bestehe, kann nachvollzogen werden. Eine strikte Anwendung der Rücksendungspflicht für sämtliche physisch eingereichten Dokumente führt allerdings zu erheblichen praktischen Problemen und widerspricht dem Geist der Digitalisierung.

1. Unverhältnismässiger administrativer Aufwand und Kosten

In der Praxis (insbesondere bei Polizei und Staatsanwaltschaften) gehen jährlich tausende Anzeigen und Mitteilungen in Papierform ein, die oft von Privatpersonen stammen. Diese Dokumente sind primär für die Behörden bestimmt; die Absender verfügen in der Regel bereits über Kopien oder die Originale. Eine gesetzlich erzwungene Rücksendung würde einen massiven, nutzlosen Postverkehr generieren, der enorme Kosten für Porti und personellen Aufwand verursacht, ohne einen prozessualen Mehrwert zu bieten. Es darf nicht sein, dass ein Gesetz zur Förderung des elektronischen Rechtsverkehrs neue, belastende Pflichten im verbleibenden Papierprozess schafft, die bisher nicht existierten.

2. Differenzierung nach dem Zweck des Dokuments

Es muss zwischen einfachen Mitteilungen und Dokumenten unterschieden werden, denen über den Informationsgehalt hinaus ein eigenständiger Beweiswert zukommt.

- Dokumente, die forensisch relevante Spuren (Unterschriften, Fingerabdrücke, DNA) enthalten oder Urkundencharakter besitzen, müssen gemäss Art. 30 Abs. 2 BEKJ ohnehin zurückbehalten werden.
- Bei einfachen Schriftstücken, Kopien oder Ausdrucken, deren Zweck sich in der Mitteilung erschöpft, sollte auf die Rücksendung verzichtet werden können, sofern die Absender dies nicht ausdrücklich verlangen.

Es wird beantragt, die Rückgabepflicht im vorstehenden Sinn einzuschränken.

Art. 22 VEKJ

Die Vorgabe, wonach die elektronischen Scans bildlich und inhaltlich mit den physischen Dokumenten übereinstimmen müssen, wird grundsätzlich unterstützt. Die Formulierung erscheint jedoch sehr weitgehend und wirft Fragen hinsichtlich ihrer praktischen Umsetzung auf. Insbesondere bleibt unklar, welche rechtlichen und

verfahrensmässigen Folgen eintreten, wenn nachträglich Abweichungen zwischen dem physischen Dokument und dem erstellten Scan festgestellt werden. Die Verordnung sollte daher präzisieren, wie mit solchen Fällen umzugehen ist und welche Anforderungen an die Übereinstimmung gestellt werden. Zudem sollten diese Anforderungen, um mit dem technischen Fortschritt Schritt halten zu können, nicht in der Verordnung, sondern in einem Anhang oder eine Departementsverordnung festgehalten werden.

Zustellung von Papierkopien elektronisch erzeugter Originaldokumente

Wir fordern die Aufnahme einer Bestimmung, die klärt, dass bei elektronisch erstellten und gesiegelten Originaldokumenten auf eine handschriftliche Unterzeichnung verzichtet werden kann, wenn diese in Papierform an Personen zugestellt werden, die noch nicht elektronisch kommunizieren.

1. Paradigmenwechsel zum elektronischen Original

Mit dem BEKJ und der VEKJ wird das elektronische Original zum Standard. Gemäss dem gesetzgeberischen Willen ersetzt das geregelte elektronische Siegel bei der elektronischen Aktenführung die eigenhändige Unterschrift. Es ist daher widersprüchlich und technisch rückständig, wenn für den Postversand eines solchen Dokuments wieder eine handschriftliche Signatur verlangt wird.

2. Vermeidung von Inkongruenzen und formalen Fehlern

Die im erläuternden Bericht angedeutete Pflicht zur handschriftlichen Unterzeichnung bei Papierversand schafft erhebliche Probleme:

- Zwei unterschiedliche „Originale“: Würde eine Papierkopie eines elektronischen Originals von Hand unterschrieben, handelte es sich formal nicht mehr um eine Kopie, sondern um ein zweites, vom elektronischen Original abweichendes Dokument. Dies kann zu Rechtsunsicherheiten führen, wenn etwa einem verteidigten Beschuldigten die elektronische (nur gesiegelte) Version und dem Privatkläger eine handschriftlich unterzeichnete Papierversion zugestellt wird.
- Beweiswert: Einer Papierkopie kommt exakt derselbe Informationsgehalt zu wie dem elektronischen Original. Bei Zweifeln an der Urheberschaft kann jederzeit das elektronische Original auf der Plattform oder am Sitz der Behörde eingesehen werden.

3. Effizienz und Wirtschaftlichkeit (Massengeschäft)

Besonders bei Behörden mit hohem Fallaufkommen (z.B. Übertretungsstrafbehörden, Staatsanwaltschaften im Strafbefehlsverfahren, Betreibungsbehörden) würde das

Festhalten an der handschriftlichen Unterschrift für den Papierversand das Rationalisierungspotenzial der Digitalisierung zunichte machen. Es ergibt keinen Sinn, Prozesse digital zu führen, um am Ende jedes Dokuments für den Versand doch wieder manuell unterzeichnen zu müssen.

4. Aufbewahrung und rechtskonforme Vernichtung

Wird die Rücksendungspflicht wie ersucht aufgehoben oder zumindest aufgeweicht, stellt sich die Frage, ob nicht ausdrücklich geregelt werden sollte, wie lange gescannte Originaldokumente nach der Digitalisierung aufzubewahren sind und ab welchem Zeitpunkt und unter welchen Voraussetzungen eine rechtskonforme Vernichtung erfolgen darf. Eine klare Regelung würde für die Vollzugsbehörden Rechtssicherheit schaffen und unterschiedliche kantonale Praktiken vermeiden.

1. Abschnitt: Verwendung von anderen Lösungen zur Übermittlung von Dokumenten

Es erscheint erforderlich, den Begriff der übrigen Behörden, also jenen, die unter das Obligatorium fallen, mit den Strafbehörden elektronisch kommunizieren zu müssen, zu definieren. Gewisse Ausnahmen sind aber denkbar, allen voran bei etablierten Schnittstellen zwischen Fachapplikationen oder bei einer Vielzahl von Schriftwechseln mit Behörden, die nicht Teil der Straf- oder Zivilprozesskette sind, wo keine Schnittstelle besteht oder wo aus Kostengründen der Rechtsverkehr über die Plattform vorgezogen wird. Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank erfolgen. Dafür braucht es nach hier vertretener Einschätzung keine Quittung. Die Protokollierung in den Logfiles des kantonalen IT-Systems genügt. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem mehrmaligen Versand von Dokumenten über eine externe Plattform klar vorzuziehen.

Art. 25 VEKJ

Es ist sicherzustellen, dass die bestehenden Prozesse von eSchKG langfristig nicht isoliert weitergeführt werden. Es sollte deshalb geprüft werden, ob entweder eine vollumfängliche technische Anbindung von eSchKG an die neue zentrale Plattform erfolgt oder in einem zweiten Schritt eine vollständige Integration des gesamten SchKG-Bereichs umgesetzt wird.

Art. 26 VEKJ

Die Möglichkeit zur elektronischen Bestätigung wird ausdrücklich begrüsst, sodass der Umweg über ein anschliessend zu scannendes Protokoll auf Papier entfällt. Es ist nicht

klar, ob elektronische (Hand-)Bestätigungen und QES kombinierbar sind, indem beispielweise eine einvernommene Partei elektronisch bestätigt und die einvernehmende Staatsanwältin eine QES anbringt. Gemäss Abs. 3 wäre das nicht möglich.

Aufhebung VeÜ-ZSSV

Wir lehnen die ersatzlose Aufhebung der Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV; SR 272.1) zum Zeitpunkt des Inkrafttretens der VEKJ ab. Diese Planung steht im Widerspruch zur gesetzlich verankerten Übergangsfrist des BEKJ und gefährdet die Kontinuität der Digitalisierung in den Kantonen, zumal die Plattformen IncaMail und PrivaSphere gemäss den in der Strafprozessordnung (StPO; SR 312.0) und Zivilprozessordnung (ZPO; SR 272) enthaltenen Übergangsbestimmungen weiterhin zum Einsatz kommen können. Die für den Betrieb und die Nutzung dieser Plattformen geltenden Bestimmungen dürfen deshalb nicht aufgehoben werden.

Mit freundlichen Grüssen

Der Präsident des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·

Numero			Bellinzona
3070	sl	0	17 giugno 2026

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Signor Consigliere federale
Beat Jans
Dipartimento federale di giustizia e polizia
Palazzo federale Ovest
3003 Berna

cornelia.perler@bj.admin.ch

Procedura di consultazione concernente il progetto di nuova Ordinanza concernente la comunicazione elettronica nei procedimenti giudiziari e amministrativi di diritto federale (OCEP)

Signor Consigliere federale,
gentili signore e signori,

vi ringraziamo per l'opportunità di esprimerci sul progetto di nuova Ordinanza in oggetto.

1. Considerazioni generali

L'avamprogetto dell'OCEP rappresenta un passaggio fondamentale per l'attuazione della legge concernente le piattaforme per la comunicazione elettronica nella giustizia (LCEG) adottata il 20 dicembre 2024 dalle Camere federali che ha formalizzato le basi legali per la creazione e l'utilizzo della piattaforma sicura e centralizzata justitia.swiss del progetto nazionale "Justitia 4.0". Gli obbiettivi generali da essa perseguiti sono condivisi dal Consiglio di Stato, che ribadisce in questa sede l'interesse a far capo alla piattaforma justitia.swiss per la comunicazione elettronica anche in ambito di giustizia amministrativa cantonale contenziosa e non contenziosa. Sulla formulazione delle singole disposizioni, il Consiglio di Stato condivide in generale le osservazioni trasmesse dalla Direzione del progetto nazionale "Justitia 4.0" alle quali qui si rimanda.

2. Osservazioni sulle singole disposizioni pertinenti OCEP

Capitolo 1: Esercizio e utilizzo di piattaforme
Sezione 3: Documenti, ricevute e sigilli
Art. 5 cpv. 2 AP-OCEP

La disposizione proposta è accolta con favore. Si ritiene importante che sulla ricevuta non figuri il nome della persona responsabile in seno all'autorità, così come proposto al cpv. 2 lett. b. Sulla ricevuta dovrebbe figurare soltanto il nome dell'autorità emittente. Il cpv. 2, lett. d, cifra 2 di questa disposizione prevede che la ricevuta di consegna stabilisce *"l'elenco dei documenti non trasmessi a causa del risultato del controllo*

antivirus, con indicazione delle loro dimensioni"; questa dicitura è però contradditoria, visto che giustamente questi documenti non sono stati trasmessi, e quindi non può essere rilasciata nessuna ricevuta a loro riguardo.

Sezione 4: Autenticazione, profili, interfacce e diritti
Art. 9 AP-OCEP

Capoverso 2 lett. b: questa disposizione si applica unicamente alle autorità incaricate della conduzione del procedimento, che figurano anche nell'elenco degli indirizzi della piattaforma centrale. Per le autorità incaricate della gestione dei procedimenti non dovrebbe essere necessario indicare un unico indirizzo postale, in quanto un'autorità può avere più sedi e più indirizzi postali (ne è un esempio il Ministero pubblico del Canton Ticino). La disposizione deve essere modificata di conseguenza.
Capoverso 3 lett. b: le aziende hanno strutture e filiali diverse, per cui il profilo digitale utilizzato non deve necessariamente coincidere con l'indirizzo postale. Quest'ultimo non apporta alcun valore aggiunto significativo nell'ambito della distribuzione digitale. Anche per le organizzazioni occorre pertanto rinunciare alla raccolta degli indirizzi postali.
Capoverso 4: la formulazione dove essere chiarita in quanto non si comprende se l'obbligo di trasmissione per via elettronica si riferisce alla persona fisica o all'organizzazione per conto della quale la persona fisica lavora. È pertanto auspicabile che l'ordinanza chiarisca il ruolo della persona responsabile in relazione alla piattaforma centrale.

Sezione 5: Protezione dei dati, sicurezza dei dati e controllo antivirus
Art. 12 AP-OCEP

Siamo favorevoli alla cancellazione automatica dei documenti dopo un periodo di tempo prevedibile. Per le ricevute, tuttavia, sembra opportuno prevedere un periodo di conservazione più lungo dei sei mesi. Le ricevute possono essere necessarie in una fase molto avanzata della procedura, ad esempio per dimostrare il rispetto di un termine o la presa di conoscenza di un determinato documento. Ovviamente, le autorità e gli avvocati devono preoccuparsi di trasferire le ricevute nei loro applicativi informatici di gestione degli incarti. Nondimeno, a causa del funzionamento della piattaforma centrale, ad esempio nel caso delle notifiche, le ricevute potrebbero non essere scaricate. In linea con il periodo di tre anni durante il quale è possibile effettuare ricerche nella corrispondenza presso la Posta svizzera, proponiamo di riformulare l'art. 12, nel senso di escludere le ricevute dal campo di applicazione del capoverso 1 e di prevedere una cancellazione (non una "distruzione"; cfr. anche il capoverso 2) automatica dopo la loro trasmissione (e non, in alternativa, anche dopo il loro rilascio).

Sezione 6: Emolumento per l'utilizzo della piattaforma centrale

Il Cantone Ticino manifesta delle riserve sul modello proposto dall'avamprogetto OCEP, in particolare per quanto riguarda la ripartizione dei costi tra Confederazione e Cantoni per il finanziamento della piattaforma. Saluta quindi con favore l'art. 21 AP-OCEP che permette il riesame della modalità di calcolo degli emolumenti. Se la proposta dell'avamprogetto di cui agli artt. 16-18 è difatti comprensibile per i primi tempi, in attesa che tutti i Cantoni introducano l'obbligo di utilizzo della piattaforma, nel seguito è verosimile la possibilità di una modifica del finanziamento in base al principio di causalità

dei costi, ossia i contributi dei Cantoni e della Confederazione dovrebbero riflettere l'effettivo utilizzo della piattaforma. Reputiamo difatti in particolare che i Cantoni con un volume di pratiche inferiore non debbano finanziare in misura sproporzionata i Cantoni con un numero importante di incarti. Anche per il Canton Ticino la trasformazione digitale della giustizia comporta già investimenti significativi a livello cantonale (gestionali, infrastrutture informatiche, applicativo informatico, interfacce, formazione del personale, ecc.). L'introduzione di contributi supplementari per justitia.swiss giusta l'avamprogetto OCEP rischia in tal senso, sul lungo termine, di generare un doppio onere finanziario per i Cantoni. Ulteriore preoccupazione per i Cantoni riguarda la necessità che gli emolumenti siano determinabili in modo chiaro e prevedibile. È difatti essenziale conoscere quali prestazioni saranno comprese nei contributi ordinari, quali costi potranno essere fatturati separatamente, come verranno adeguati gli emolumenti in futuro. Quanto all'art. 16 AP-OCEP, chiediamo di specificare al capoverso 2 che la quota dei Cantoni è ripartita tra i Cantoni che sono membri dell'ente proporzionalmente alla loro popolazione residente permanente *"al 1. gennaio dell'anno precedente a quello per il quale è dovuto l'emolumento"* e non "nel momento della fissazione dell'emolumento".

Capitolo 2: Digitalizzazione di documenti fisici
Art. 22 AP-OCEP

Il Consiglio di Stato, allineandosi alla presa di posizione della Direzione del progetto Justitia 4.0, constata che l'AP-OCEP non contiene disposizioni relative all'eventuale rinvio dei documenti fisici (cartacei) ai mittenti non iscritti sulla piattaforma e che tale lacuna andrebbe opportunamente colmata. Parimenti, perseguendo la digitalizzazione delle procedure l'obiettivo di semplificare e rendere più efficiente l'attività giudiziaria, senza tuttavia introdurre nuovi oneri formali o obblighi procedurali che non trovano riscontro nella procedura cartacea, come proposto dalla Direzione del progetto Justitia 4.0, postuliamo l'inserimento di una nuova normativa che chiarisca il rinvio di documenti fisici da parte delle autorità. Condividiamo inoltre l'inserimento di una nuova normativa nell'OCEP concernente la notifica di copie cartacee di documenti originali prodotti elettronicamente, come proposto e motivato dalla Direzione del progetto Justitia 4.0 nella propria presa di posizione.

Capitolo 3: Trasmissione elettronica al di fuori di una piattaforma secondo la LCEG
Sezione 1: Utilizzo di altre soluzioni per la trasmissione di documenti
Art. 23 AP-OCEP

Ribadendo il principio secondo cui la digitalizzazione non deve introdurre obblighi più gravosi rispetto alla procedura cartacea, chiediamo di consentire espressamente la trasmissione elettronica mediante modifica dei diritti di accesso a una banca dati comune e di rinunciare al requisito della marca digitale sincronizzata previsto alla lett. b, ritenuto non necessario alla luce delle esigenze del CPC e del CPP.

Art. 24 AP-OCEP

Il Consiglio di Stato ritiene che il titolo dell'art. 24 sia eccessivamente ampio e potenzialmente fuorviante, poiché la disposizione riguarda unicamente le comunicazioni effettuate nell'ambito di procedimenti disciplinati dal CPC, dal CPP e dalla LAV. Chiediamo di chiarire la nozione di «altre autorità» soggette all'obbligo di comunicazione

elettronica, in particolare per quanto concerne gli enti di diritto pubblico che non esercitano funzioni di pubblica autorità. Le eccezioni previste dalla norma sono condivisibili nei casi in cui, per ragioni operative, tecniche o economiche, risulti preferibile una comunicazione diretta tra autorità o tramite interfacce dedicate, anziché attraverso la piattaforma centrale. Ciò può riguardare, ad esempio, autorità fiscali o migratorie, grandi aziende di trasporto, istituti di medicina legale o determinate autorità federali. Per quanto concerne i requisiti tecnici e documentali, il Consiglio di Stato ritiene che essi debbano essere allineati a quelli previsti dall'art. 23 e non essere più restrittivi. In particolare, non vi è alcuna giustificazione per imporre obblighi supplementari di documentazione della trasmissione, poiché l'art. 103c cpv. 2 CPP, a differenza dell'art. 103b cpv. 2 CPP, non prevede requisiti specifici in tal senso. Anche in questo ambito occorre evitare che la digitalizzazione introduca formalità od oneri amministrativi più gravosi rispetto a quelli esistenti nella procedura tradizionale.

Capitolo 4: Disposizioni finali
Abrogazione dell'Ordinanza sulla comunicazione per via elettronica nell'ambito di procedimenti civili e penali nonché di procedure d'esecuzione e fallimento (OCE-PCPE)

L'abrogazione dell'OCE-PCPE trasferisce di fatto ai Cantoni la responsabilità di garantire canali elettronici sicuri per numerosi procedimenti amministrativi, con il rischio di generare costi aggiuntivi, soluzioni eterogenee e una minore uniformità a livello nazionale rispetto agli obiettivi perseguiti dalla digitalizzazione della giustizia e dell'amministrazione. Il Cantone propone che la Confederazione mantenga, almeno per un periodo transitorio, la possibilità di utilizzare fornitori di recapito elettronico riconosciuti alternativi a justitia.swiss (quali IncaMail o soluzioni equivalenti), oppure metta a disposizione dei Cantoni una soluzione federale interoperabile utilizzabile anche per i procedimenti amministrativi non coperti dalla piattaforma justitia.swiss, qualora quest'ultima non potesse assorbire anche i procedimenti amministrativi cantonali contenziosi e non. In alternativa, si chiede che l'OCEP o il relativo rapporto esplicativo precisino le modalità con cui i Cantoni potranno adempiere all'obbligo di garantire canali elettronici sicuri per i procedimenti amministrativi esclusi dall'ambito di justitia.swiss, nonché le condizioni tecniche minime e le interfacce necessarie per assicurare l'interoperabilità a livello nazionale.

Ulteriori osservazioni
Incarti ibridi

Il mantenimento della possibilità per le parti non rappresentate di comunicare in forma cartacea costituisce una scelta coerente con il principio di accesso alla giustizia e con l'assenza, nel diritto processuale svizzero, di un obbligo generalizzato di patrocinio legale. Tale impostazione comporta tuttavia che, anche dopo l'introduzione della piattaforma justitia.swiss, coesisteranno inevitabilmente modalità di comunicazione analogiche e digitali. Per garantire un funzionamento efficiente del sistema, sarebbe opportuno che l'ordinanza o il rapporto esplicativo precisassero maggiormente le modalità di gestione degli atti trasmessi da utenti non soggetti all'obbligo di comunicazione elettronica, disciplinando in particolare l'integrazione dei documenti cartacei nel fascicolo elettronico e la ripartizione delle relative responsabilità organizzative.

Vogliate gradire, Stimato Consigliere federale, gentili signore e signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente
Claudio Zali

Il Cancelliere
Arnoldo Coduri

Copia a:
- Direzione del Dipartimento delle istituzioni (di-dir@ti.ch)
- Divisione della giustizia (di-dg@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch)
- Comando della Polizia cantonale (polizia-segr@polca.ti.ch; servizio.giuridico@polca.ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet



Landammann und Regierungsrat des Kantons Uri

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Vernehmlassung

Sehr geehrter Herr Bundesrat
Geschätzte Damen und Herren

Mit Schreiben vom 13. März 2026 hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) den Urner Regierungsrat im Rahmen eines Vernehmlassungsverfahrens eingeladen, zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung zu nehmen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und äussern uns dazu wie folgt:

Wir begrüssen die Vorlage, die der Umsetzung des neuen Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) dient. Sie schafft einheitliche technische und organisatorische Regeln für die elektronische Kommunikation in allen Straf-, Zivil- und Verwaltungsgerichtsverfahren des Bundes. Auch die vorgesehene Gebührenerhebung ist grundsätzlich zu begrüssen, da sie eine stabile Finanzierung der digitalen Justizinfrastruktur sicherstellt und die Kosten solidarisch zwischen Bund und Kantonen verteilt. Im Übrigen verzichten wir auf eine einlässliche Stellungnahme.

Sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren, wir danken Ihnen für die Gelegenheit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 19. Juni 2026

REGIERUNGSRAT DES KANTONS URI

Im Namen des Regierungsrats

Der Landammann	Der Kanzleidirektor
Daniel Furrer	Roman Balli

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Monsieur le Conseiller fédéral
Beat Jans
Chef du Département fédéral de justice et police
3003 Berne

Envoi par courriel (PDF et Word) à :
cornelia.perler@bj.admin.ch

Réf. : 26_COU_3386

Lausanne, le 17 juin 2026

Consultation fédérale : avant-projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,

Le Conseil d'Etat du Canton de Vaud vous remercie d'avoir sollicité son avis sur le projet d'ordonnance cité en titre. Après avoir mené une consultation auprès des organismes concernés du Canton, il a l'honneur de vous faire part de ses déterminations. L'avant-projet vise à mettre en œuvre la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ ; RS 172.023 ; RO 2025 583). Il précise à cet effet plusieurs aspects essentiels tels que la procédure d'autorisation pour la plateforme centrale et les autres plateformes, les émoluments consécutifs à l'utilisation par les membres de la corporation publique à créer et les non-membres, l'authentification des utilisateurs, le format des communications, la numérisation des documents remis sur papier et l'attestation de l'exactitude des procès-verbaux dans les procédures pénales et militaires.

Le Conseil d'Etat soutient pleinement les objectifs poursuivis par la LPCJ et le projet Justitia 4.0, qui constituent une étape importante dans la modernisation de la justice suisse et dans la transition vers des procédures plus efficientes, plus accessibles et davantage adaptées aux réalités numériques contemporaines.

Toutefois, plusieurs dispositions de l'avant-projet d'ordonnance nécessitent encore des clarifications et des adaptations importantes afin de garantir la sécurité informatique des échanges, la sécurité juridique des procédures, la faisabilité opérationnelle pour les cantons et les autorités concernées ainsi qu'une mise en œuvre proportionnée et durable.

En particulier, les exigences relatives à la cybersécurité (standards de chiffrement, gestion des clés cryptographiques, détection des menaces et conformité aux exigences de la loi fédérale sur la sécurité de l'information) devraient être renforcées et davantage explicitées dans l'ordonnance.

Par ailleurs, certaines dispositions apparaissent excessivement rigides ou insuffisamment adaptées aux réalités pratiques des autorités judiciaires et administratives. Il apparaît essentiel de préserver une approche pragmatique et fédéraliste dans la mise en œuvre de la plateforme justitia.swiss, en laissant au DFJP et aux autorités compétentes la possibilité d'adapter les exigences techniques à l'évolution rapide des technologies et des risques numériques.

Sous réserve des adaptations proposées dans les commentaires techniques qui vous sont remis en annexe, l'avant-projet paraît constituer une base solide pour le développement d'une justice numérique suisse sécurisée, efficace et respectueuse des réalités institutionnelles cantonales.

En conclusion, s'il estime que l'avant-projet mis en consultation mérite encore un certain nombre d'ajustements, le Conseil d'Etat peut le soutenir dans sa globalité.

Vous remerciant de l'accueil qui sera réservé aux observations du Canton de Vaud, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre considération distinguée

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER.
Christelle Luisier Brodard	Michel Staffoni

Annexe

- Commentaires techniques

Copies

- Office des affaires extérieures
- DAJ – Direction général des affaires institutionnelles et des communes

Annexe à la réponse du Conseil d'Etat à la procédure de consultation fédérale

relative à l'avant-projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Commentaires techniques

Remarques d'ordre général

La loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPJC) ne prescrit rien en matière de clés internes de la plateforme (TLS, chiffrement au repos, clés d'API). En particulier, des sujets tels que les modules matériels de sécurité, la rotation, le séquestre et la révocation ne sont aucunement traités et il paraîtrait utile de les aborder dans l'OCEP ou, à tout le moins, dans une ordonnance du DFJP.

À l'article 25, alinéa 2, LPJC, il est mentionné que l'octroi d'une autorisation d'exploiter une plateforme nécessite que son code source soit disponible en libre accès, sous une forme adéquate. L'OCEP ne précise cependant pas ce qui constitue une forme adéquate et quelles doivent être les modalités du libre accès (licence, dépôt, maintien de l'accès sur la durée, etc.). Ces éléments mériteraient d'être traités, soit dans l'OCEP, soit dans une ordonnance départementale.

Article 1	Selon notre interprétation, l'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral et **ne s'applique donc pas aux cantons**. La valeur ajoutée de l'alinéa 3 n'est pas évidente, étant donné qu'en cas de divergence, une loi prévaudrait de toute façon sur la présente ordonnance.
Article 2	Les conditions applicables aux plateformes semblent appropriées. Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre c, devrait être fixée dans une annexe à la présente ordonnance ou dans une ordonnance du DFJP. **La fonction de suppression visée à l'alinéa 1, lettre d, est une fonctionnalité** qui, le cas échéant, devrait être réglementée dans la section 3 de la présente ordonnance. Par ailleurs, la formulation de cette disposition est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport à la page 11, la fonction de suppression efface l'autorisation individuelle accordée, mais pas le document en tant que tel. Il conviendrait également, s'agissant de la suppression, de faire la distinction entre les autorités et les autres utilisateurs. L'indication à la lettre b selon laquelle les documents sur la plateforme sont chiffrés selon les normes techniques de l'administration fédérale paraît trop vague. L'OCEP devrait citer explicitement le cadre NCSC et/ou les séries eCH applicables, avec un cycle de révision défini. En outre, la question post-quantique n'est pas abordée. Plusieurs aspects importants sont couverts par le renvoi de l'article 13 à la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (LSI ; RS 128). Il pourrait cependant également être utile de renforcer explicitement le lien avec cette autre loi en mentionnant au présent article 2 que les plateformes doivent être conformes à la catégorie de sécurité « protection élevée » de la LSI (art. 5 LSI)

Article 4	Le présent projet utilise – à l'instar de la LPCJ – le terme « document » plutôt que « fichier » (cf. message LPCJ, p. 20), en invoquant que le terme « fichier » est un terme trop technique pour être utilisé dans la loi. Le terme « fichier » est préférable dans l'ordonnance, dans la mesure où il s'agit d'aspects techniques des pièces transmises. *Al. 1* Nous sommes favorables à la définition du format PDF/A pour les documents des autorités et des formats PDF et PDF/A pour les autres participants à la procédure. *Al. 2* Dans de nombreux cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Dans ces cas, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. Si les parties soumettent leurs pièces jointes au format PDF, la conversion par les autorités judiciaires n'est plus nécessaire et toutes les parties disposent du même document. La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si, en règle générale, les documents sont disponibles au format PDF, cela permet un traitement rapide par les avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers. Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. De plus, le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées. Dans certains cas particuliers, le format PDF ne permet pas de restituer suffisamment le contenu informatif d'un document. On peut penser par exemple à des enregistrements audio ou vidéo, à des vidéosurveillances multipistes de tunnels ou à des enregistrements provenant de voitures électriques. Dans ces cas, le DFJP devrait définir quels formats de fichiers peuvent être transmis directement via la plateforme. Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format Zip. Les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centrale. L'alinéa 2 devrait donc être libellé comme suit : *[2] ~~Les annexes peuvent être remises dans n'importe quel format~~ Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine.* Un risque critique en termes de cybersécurité doit toutefois être relevé ici. En effet, en permettant que les fichiers puissent être transmis dans leur format d'origine, quel qu'il soit, les utilisateurs de la plateforme seront

	exposés à des fichiers dont la simple ouverture pourrait déclencher l'exploitation d'une vulnérabilité. *Al. 3 et 4* Le fait d'accepter des archives compressées dans une plateforme dont la sécurité repose sur un contrôle antivirus revient à contourner ce mécanisme par construction, ce qui est extrêmement problématique. En effet, un ZIP protégé par mot de passe est opaque à tout antivirus. L'expéditeur communique le mot de passe par un autre canal, le destinataire ouvre l'archive sur son poste, et la charge s'exécute dans l'environnement cantonal. C'est l'exemple-type de mode opératoire documenté dans les campagnes de rançongiciel qui ciblent régulièrement les administrations européennes (p.ex. : Emotet et QakBot). À cette menace s'ajoutent également les « zip bombs » (ratio de compression extrême conçu pour saturer le destinataire), les archives imbriquées, les doubles extensions et le format 7z dont la compression LZMA2 complique l'analyse. La sélection proposée de formats de fichiers est adéquate, mais le niveau de norme retenu est critiquable. La définition des formats que les autorités chargées de la procédure doivent traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP. La liste des formats de documents pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.). Il est nettement plus facile de gérer cela dans une annexe que dans le corps de la présente ordonnance. Les alinéas 3 et 4 devraient donc être libellés comme suit : *[3] ~~L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :~~Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour qu'elle puisse la transmettre dans un format défini par l'autorité.* *~~a. documents écrits : PDF, PDF/A ;~~ ~~b. images : BMP, GIF, JPEG, PNG ;~~ ~~c. fichiers audio : MP3, OGG, WAV ;~~ ~~d. fichiers vidéo : AVI, MOV, MKV, MP4 ;~~ ~~e. fichiers d'archives : ZIP, 7z.~~* *[4] ~~Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée~~ Le DFJP définit les formats de fichiers à transmettre via la plateforme.* *[5] ~~L'autorité qui dirige la procédure fixe un délai approprié.~~*
Article 5	Nous sommes favorables à la réglementation proposée. Il est important que **le nom de la personne responsable d'une autorité**, au sens de l'alinéa

	2, lettre b, **ne figure pas** dans la quittance. Seul le nom de l'autorité devrait apparaître sur la quittance. Un résultat positif lors du contrôle antivirus visé à l'alinéa 2, lettre d, chiffre 2, constitue un motif possible de rejet par la plateforme, mais pas le seul. La taille ou le format du fichier peuvent également en être la cause. L'alinéa 2, lettre d, chiffre 2 précise que les documents qui n'ont pas été transmis sont mentionnés dans la quittance de réception. Cette disposition comporte une erreur logique. Les documents non transmis ne peuvent pas figurer sur la **quittance de réception**, puisqu'ils n'ont justement **pas été transmis**. Par conséquent, la quittance ne peut contenir la valeur de hachage de fichiers qui n'ont pas été transmis. Si la plateforme ne parvient pas à transmettre un ou plusieurs documents, l'expéditeur reçoit un message de la plateforme, mais pas de quittance. Le chiffre 2 doit donc être supprimé. *[2] Les quittances comportent en particulier les données suivantes :* *a. le type de quittance ;* *b. le nom de l'expéditeur, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit;* *c. le nom du destinataire ou de son entreprise et son adresse sur la plateforme ;* *d. pour la quittance de réception :* *1. la liste des documents transmis, leur taille et leur valeur de hachage,* *~~2. laliste des documents qui n'ont pas été transmis en raison du résultat du contrôle antivirus, avec indication de leur taille,~~* *~~3.~~2.le moment de la transmission à la plateforme;* *e. …* *f. …* *g. …* Les plateformes doivent à l'avenir pouvoir également transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car les fichiers XML, pour des raisons techniques, ne peuvent pas être cachetés.
Article 6	Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement. La plateforme au contraire appose un cachet **après** la transmission via la plateforme, sur la quittance émise sur la base de l'article 5. L'article 6 règle **l'apposition d'un cachet sur les documents** par l'autorité dirigeant la procédure **avant leur transmission via une plateforme** (art. 22 al. 2 LPCJ). Le projet mentionne que lorsque plusieurs documents sont transmis, il suffit qu'un seul de ces documents soit muni d'un cachet, ce qui est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examinée indépendamment de la plateforme.

	Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Par ailleurs l'obligation d'apposer un cachet imposée aux autorités qui dirigent la procédure ainsi qu'aux autorités qui y participent est en contradiction avec le concept technique de la plateforme centralisée. Pour diverses fonctionnalités de la plateforme centralisée, **la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure** est essentielle. Ainsi, seules les autorités qui dirigent la procédure peuvent procéder à des notifications. Seules les adresses des autorités qui dirigent la procédure sont visibles pour les tiers dans le répertoire public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités participant à la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations et particuliers et indépendamment d'une procédure (judicaire). Cela ouvrirait la plateforme à toute communication électronique entre autorités, pour laquelle la LPCJ n'offre toutefois pas de base légale suffisante. L'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires. **Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents.** L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision incidente ou le jugement d'une autorité qui dirige la procédure crée des droits et des obligations. Ceux-ci produisent leurs effets au-delà de la procédure en cause. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète ou de la plateforme centralisée, si le document en question est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités agissent de manière autoritaire. **Les autorités participant à la procédure ne peuvent en revanche pas être tenues d'apposer un cachet électronique sur leurs documents.** Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent généralement pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante. Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante pour équiper l'ensemble des autorités suisses d'un cachet électronique. L'instauration généralisée d'un cachet électronique

	entraînerait pour les cantons un effort organisationnel considérable et des coûts importants. Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond pas au concept de la LPCJ, laquelle ne prescrit aucune fonctionnalité permettant à la plateforme de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre via la plateforme. Il serait cependant utile de préciser comment les autorités peuvent signer des documents qui, selon la jurisprudence actuelle, doivent porter la signature de leur auteur, comme les expertises (BSK StPO-Heer, art. 187 N 1). Dans le cas des instituts de médecine légale ou de l'Institut fédéral de métrologie METAS, par exemple, ces expertises peuvent tout à fait être réalisées par des autorités ou, à tout le moins, par des « services administratifs ». Dans ces cas, l'identité de l'expert qui établit l'expertise est déterminante, raison pour laquelle la signature électronique qualifiée (contrairement au commentaire de l'art. 22 LPCJ dans le message, FF 2023 679ss, p. 30) devrait probablement continuer à s'appliquer à l'avenir. Il est important de souligner la différence entre l'envoi et la consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents lors de la consultation en ligne du dossier.
Article 7	Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement (art. 6). La plateforme, en revanche, appose son cachet **après** la transmission sur la plateforme, sur la quittance de réception émise, qui est régie par l'article 5. **Al. 1** Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la **quittance, jamais le document transmis.** Dans le cas de la plateforme centralisée, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit : *[1] Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.* **Al. 2**

	L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. **L'alinéa. 2 doit donc être supprimé**. ~~*[2] Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.*~~
Article 9	**Al. 2** Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, car une autorité peut disposer de plusieurs sites. La disposition doit être adaptée en conséquence : *[2] Les profils des autorités comprennent au moins les données suivantes :* *a. le nom de l'autorité ;* ~~*b. l'adresse postale ;*~~ *b ~~c~~. le nom du cachet.* **Al. 3, let. a** La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et administratif. Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs doit être considéré comme critique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques. *[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :* *pour les personnes physiques : le prénom, le nom, la date de naissance ~~et l'adresse postale~~ ;* **Al. 3, let. b** Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique**. Il convient donc de renoncer à l'adresse postale également pour les organisations.** L'alinéa 3 devrait donc être formulé comme suit: *[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :* *a. pour les personnes physiques : le prénom, le nom, <u>et</u> la date de naissance ~~et l'adresse postale~~ ; …*

	b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse~~ ~~postale.~~* **Al. 4** Le sens de cet alinéa n'est pas compréhensible. Il n'est pas clair s'il s'agit du profil d'une organisation ou d'un particulier. Une clarification semble indiquée. Le rapport mentionne la personne responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.
Article 10	Cet article permet aux utilisateurs de la plateforme de connecter leurs systèmes à celle-ci via une interface et d'octroyer des droits de représentation à leurs collaborateurs. Cela se fait par l'intermédiaire d'un utilisateur technique qui reçoit un mot de passe numérique (token). La réglementation proposée est donc saluée.
Article 11	**Art. 11 ~~Attribution~~ Confirmation et retrait de droits** La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait de parler de « confirmation » plutôt que d'« attribution ». Nous sommes favorables à la variante proposée à l'alinéa 2.
Article 12	**Problématique** L'article 12 du projet d'ordonnance OCEP prévoit que les documents et les quittances soient automatiquement supprimées de la plateforme à l'expiration d'un délai de six mois. Nous sommes favorables à la suppression automatique des documents après un délai raisonnable, car la plateforme est conçue comme une « boîte aux lettres » et non comme un moyen d'archivage à long terme. Il semble cependant opportun, en ce qui concerne les quittances, de prévoir un délai plus long. Les quittances peuvent encore être nécessaires très tard dans la procédure, par exemple pour prouver le respect d'un délai ou la prise de connaissance d'un document donné. Bien entendu, les autorités doivent veiller à transférer les quittances dans leurs propres logiciels de gestion d'affaires. Cependant, le fait que, en raison du fonctionnement de la plateforme centralisée, elles ne soient pas classées dans les dossiers d'une procédure, par exemple en cas de notifications, peut conduire à ce que le téléchargement des quittances ne soit pas effectué. Contrairement aux requêtes et aux notifications, qui peuvent être renvoyées depuis les systèmes sources, les quittances générées par la plateforme elle-même seraient dans ce cas déjà perdues au bout de six mois. A ce stade-là, une procédure n'est souvent pas encore terminée. Les quittances peuvent également contenir des données personnelles (telles que les noms des parties à la procédure), ce qui, dans le contexte des procédures judiciaires, peut même en faire des données personnelles particulièrement sensibles. Cependant, ces données, tout comme les pièces du dossier elles-mêmes, bien plus sensibles, sont stockées de manière sécurisée sur la plateforme. À cela s'ajoute le fait que les quittances constituent également de très petites quantités de données qui ne nécessitent pas de stockage supplémentaire important, même si elles restent disponibles longtemps sur la plateforme.

	Solution proposée Il est proposé ici de modifier ou de compléter l'article 12 AP-OCEP en s'alignant sur le délai de suppression de trois ans pendant lequel la Poste suisse permet d'effectuer des recherches dans le courrier. En français le fait que la suppression est automatique manque dans le libellé de l'alinéa 1 et devrait être complété comme suit: *Art. 12 Durée maximale de conservation des documents et des quittances* *[1] Les documents ~~et les quittances~~ enregistrés sur une plateforme sont automatiquement ~~détruits~~supprimés six mois après leur réception ~~ou leur délivrance~~.* *[2] Lorsque des documents peuvent être consultés, l'autorité qui dirige la procédure fixe le délai pendant lequel ils sont disponibles sur la plateforme. Passé ce délai, ils sont automatiquement supprimés ~~détruits~~.* *[3] Les quittances sont automatiquement supprimées trois ans après leur délivrance.* **Al. 2** Nous sommes favorables à la solution proposée. Il n'est pas nécessaire de prévoir une prolongation du délai dans l'ordonnance, car l'autorité peut ordonner une deuxième consultation du dossier avec les mêmes pièces.
Article 13	La disposition proposée renvoie à la section 3 ; la mention du chapitre pertinent (2 ?) fait défaut et devrait être ajoutée.
Article 14	Tout d'abord, l'approche « antivirus unique sur fichier statique » nous paraît faible. Par ailleurs, la notion d'« antivirus » telle que mentionnée dans l'ordonnance est dépassée car elle renvoie à une catégorie d'outils spécifique, historiquement basée sur des signatures. Une formulation plus large, telle que « systèmes de détection et d'analyse des menaces », couvrant des approches modernes (analyse comportementale, sandboxing, etc.), devrait lui être substituée. Le sandboxing pourrait constituer une mesure compensatoire pour les fichiers volumineux (plus grands que 64 Mo) ou les formats à haut risque (archives simples et protégées par mot de passe), tout en limitant les coûts d'analyse en ne faisant pas de contrôle automatiquement. Ensuite, du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants. 1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse atteindrait sa limite (espace de stockage, etc.), interromprait l'analyse et le processus d'analyse pourrait prendre tellement de temps que le respect des délais serait compromis en cas de soumission dans l'urgence. 2. Analyse limitée des fichiers volumineux : un fichier qui dépasse la taille maximale fixée est divisé en blocs gérables aux fins de l'analyse de logiciels malveillants, lesquels sont ensuite analysés individuellement. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont

répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :
   - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
   - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analysés pour détecter de logiciels malveillants, car ils sont chiffrés.
   - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
   - En raison des mesures de protection, des fichiers sont rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».
     Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail classique, Dropbox…). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et **cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, respectivement avant et après leur transmission via la plateforme**. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus.

Al. 1

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne devrait pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra fortement du logiciel chargé de la division et de la

	vérification. Cette limite évoluera également de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels, et devrait pouvoir être facilement adaptée. L'alinéa 1 devrait donc être libellé comme suit : [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets à~~ effectuent un contrôle antivirus.* **Al. 2** La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants peut (et devrait) être facilement augmentée par les exploitants de la plateforme en fonction des possibilités techniques et de l'expérience opérationnelle croissante. **L'alinéa 2 doit donc être supprimé**. ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~ **Al. 4** Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est essentielle selon nous. La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond. L'alinéa 4 devrait donc être libellé comme suit : [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels. **Al. 5** Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, il ne s'agit manifestement pas d'une quittance, puisqu'aucun document n'a été transmis (voir les commentaires aux art. 5, al. 2, let. d, ch. 2, ci-dessus).
Article 15	Les versions allemande et française ont été comparées et harmonisées ; cela vaut également pour la cohérence terminologique des notions y figurant. Pour plus de clarté, l'alinéa 1 a été scindé en deux (nouveaux) alinéas. La référence à la planification financière triennale pour la fixation du montant total de l'émolument pour trois ans est saluée. Cette approche fournit une base prévisible et réaliste pour l'émolument fixé annuellement selon la clé de répartition figurant à l'article 16. Au surplus, la mesure corrective prévue à l'alinéa 4 garantit une capacité d'adapter l'émolument si nécessaire. Le texte suivant est proposé : *[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement de la plateforme*

	centralisée ~~-~~et permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public~~. Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~. *[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.* *[3]Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.* *~~3~~4 Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~'il~~ ne couvrent pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.*
Article 16	Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération, mais pas pour les procédures administratives de première instance. La part fédérale de 10 % est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen. Nous sommes favorables à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixe le montant annuel des émoluments ; il tient compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17). La formulation suivante est proposée : *[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :* *a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;* *b. tribunaux de la Confédération : 5 % ;* *c. cantons : 90 %.* *[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû ; est déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.* *[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.*

Article 19	L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du Code des obligations s'appliquent par analogie. Il est donc proposé d'adopter le libellé suivant pour cette disposition : *[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.* *[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.* *[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.*
Article 21	Nous sommes favorables à la révision du mode de calcul de l'émolument proposée.
Article 22	Cette disposition concerne toutes les autorités qui mènent des procédures dont le droit procédural est déclaré applicable par la LPCJ (art. 2 LPCJ). Pour les cantons, ce sont donc le Code de procédure civile, la loi sur l'aide aux victimes et le Code de procédure pénale qui priment. Le format PDF/A prescrit à l'alinéa 2 facilite l'archivage des dossiers judiciaires. Il n'est toutefois pas certain que ce format puisse être facilement traité par les applications judiciaires cantonales, qui sont très différentes les unes des autres. L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. La profondeur d'au moins 8 bits et une résolution de 300 dpi semblent judicieuses s'agissant de texte mais pourraient être insuffisantes pour des pièces visuelles plus complexes (ex : photos). Il convient de noter qu'avec une résolution de 300 dpi, la taille du fichier est quatre fois supérieure à celle obtenue avec une résolution de 150 dpi.
Article 22*a* (nouveau)	**Problématique** Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est indiqué qu'il a été renoncé à intégrer dans l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (AP-OECP) une disposition relative à l'interprétation restrictive de l'article 30 LPCJ, car il n'y avait plus de marge de manœuvre légale à cet effet. Cette constatation se réfère à l'interprétation de la notion de « documents » contenue dans l'article 30 LPCJ, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents. Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas encore dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent tout à fait une marge d'interprétation des dispositions de la LPCJ dans le sens de leur objectif législatif.

	En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme « justitia.swiss ». Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur. Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, une loi visant à introduire les communications judiciaires électroniques instaurera de nouvelles obligations de renvoi dans le processus papier, qui n'existaient pas encore dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur. Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc très majoritairement jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine. Même dans le cas, plutôt rare, où des divergences surgiraient a posteriori quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité. La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ. L'article 30, alinéa 2 LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce. En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraîne une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur. **Solution proposée**

	Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2 LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il semble nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable. […]***Art. 22a*** *Renvoi des documents physiques* *Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.*
Article 22*b* (nouveau)	**Problématique : Comment joindre les personnes qui ne sont pas joignables sur la plateforme ?** Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est précisé que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k du nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (…) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, du nCPC contient une disposition similaire pour les décisions des tribunaux civils. L'article 22 concrétise l'article 29 LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme. Toutefois, lorsque des particuliers ne souhaitent pas s'inscrire sur une plateforme de transmission électronique, ils conserveront à l'avenir le droit de se voir remettre un exemplaire papier des communications et des décisions. En particulier, les autorités pénales chargées des contraventions et les services des ordonnances pénales des ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers, parce que, selon l'interprétation (désormais abandonnée) des dispositions procédurales applicables par l'ordonnance relative à la LPCJ, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers pouvant être gérés par voie électronique. C'est notamment

	dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore. Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s'agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d'interpréter l'exigence de signature de manière si restrictive qu'elle freine tout progrès. Il ressort de l'article 22, alinéa 2 LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L'exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l'authentification à l'aide d'un moyen d'identification électronique reconnu ainsi que l'apposition d'un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023 ; FF 2023 679ss, remarques préliminaires concernant l'art. 22, p. 30). Il en résulte que le cachet électronique réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n'y a donc plus de place pour un recours à l'article 14 CO dans le champ d'application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ). **Solution proposée** Il convient certes de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendues lorsqu'elles sont envoyées **sous forme d'original** sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi. Aujourd'hui déjà, il est d'usage courant auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une **nouvelle obligation est créée dans le monde analogique**. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique. Cela ne peut avoir été l'intention du législateur. En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), qui reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des

	doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier. La solution proposée présenterait l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier. Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b: ***Art. 22b*** *Notification de copies papier de documents créés par voie électronique* *Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.* Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet de l'OCEP, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.
Article 23	Cette disposition concrétise l'article 128b, alinéa 2 CPC, l'article 103b, alinéa 2 CPP et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI). Nous partons du principe que cette disposition vise la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'enquête du ministère public à la police judiciaire ou lors de la transmission des résultats d'actes d'enquête que la police transmet au ministère public.

	Un deuxième champ d'application est la chaîne de procédure civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours. La transmission physique des dossiers entre les autorités pénales s'effectue actuellement encore souvent par la poste, par courrier interne ou par coursier. La mission confiée à la police pour une mesure d'instruction est généralement formulée par écrit, mais ni la date exacte ni la réception ne sont consignées séparément. Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faudrait toutefois appliquer d'autres exigences que pour la communication via la plateforme. La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, nous estimons qu'aucune quittance n'est nécessaire. L'enregistrement dans les logfiles du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe. L'article 23 devrait être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.
Article 24	L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils, ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. la consultation relative à l'art. 6 OECP). Une incertitude subsiste à cet égard, notamment en ce qui concerne les corporations de droit public qui n'agissent pas dans l'exercice de la puissance publique. Cette disposition précise les exceptions prévues à l'article 128c, alinéa 2 CPC, à l'article 103c, alinéa 2 CPP et à l'article 8d, alinéa 2 LAVI. Ces exceptions sont justifiées lorsque, dans le cadre de procédures civiles ou pénales, un grand nombre de communications avec les autorités sont nécessaires, communications qui ne font pas partie de la chaîne de procédure pénale ou civile, et lorsque la communication directe, par exemple via une interface, est préférable aux communications électroniques dans le domaine judiciaire via la plateforme, notamment pour la transmission de métadonnées ou pour des raisons de coût. Dans le cadre de la procédure pénale, on peut penser par exemple aux autorités fiscales

	ou de migration, ou encore aux grandes entreprises de transport ou aux instituts de médecine légale, qui devraient également relever de la notion d'autorité. Il en va de même pour certaines autorités fédérales telles que l'OFDF. Les conditions devraient s'inspirer de l'article 23 et ne pas aller au-delà. En tout état de cause, on ne voit pas pourquoi l'article 24 prévoit des exigences plus strictes, étant donné que l'article 103c, alinéa 2 CPP – contrairement à l'art. 103b, alinéa 2 CPP, qui prévoit l'enregistrement du moment de transmission et la protection du dossier contre toute modification et toute consultation non autorisée – n'impose aucune exigence quant à la documentation d'une transmission.
Article 28	Le financement du projet Justitia 4.0, qui met en place la plateforme pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.
Abrogation OCEI-PCPP	En raison de l'abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite, IncaMail et PrivaSphere ne pourront plus être utilisés dans les procédures engagées après l'entrée en vigueur de l'ordonnance. Il appartient donc aux cantons de choisir et de mettre à disposition des canaux appropriés pour les procédures administratives qui ne peuvent pas être traitées via la plateforme justitia.swiss.

Conseil d'Etat
Staatsrat
CP 670, 1950 Sion

CANTON DU VALAIS
KANTON WALLIS

2026.02464

P.P. CH-1951 Sion A-PRIORITY Poste CH SA

Monsieur
Beat Jans
Conseiller fédéral
Chef du Département fédéral de justice et police
Palais fédéral ouest
3003 Berne

Notre réf. MT
Date 17 JUIN 2026

Consultation - Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,

Le Conseil d'Etat valaisan a pris connaissance de l'avant-projet d'ordonnance cité en exergue et vous remercie de l'avoir consulté. Il vous communique ci-après sa détermination.

Notre canton a été associé à un groupe de travail, lequel a élaboré une prise de position concernant l'AP-OCEP annexée à la présente. Le Conseil d'Etat constate que le projet présente de nombreuses faiblesses auxquelles il s'agit de remédier dans le sens de cette détermination à l'exception de la suppression de la collecte de l'adresse postale des personnes physiques (art. 9 al. 3 let. a AP-OCEP) utile à la fixation du for en procédure pénale.

En outre, votre département peut modifier les exigences et les interfaces sans restriction selon l'article 2 AP-OCEP. Chaque utilisateur de la plateforme devra donc observer les changements techniques imprévisibles, supporter des coûts d'intégration continus et assumer des risques de rupture applicative. Votre département devrait publier un cadre d'architecture et d'interopérabilité contraignant définissant les protocoles, les formats d'échange, les mécanismes de versionnement, la gouvernance des API, les exigences de compatibilité, la politique de dépréciation ainsi que les exigences minimales en matière de résilience, de supervision et de continuité de service.

Nous profitons de vous informer que le Grand Conseil valaisan a franchi une étape importante en vue de la numérisation de la justice en acceptant le 4 mai 2026 la loi d'adhésion à la convention entre la Confédération et les cantons sur la corporation « justitia.swiss » (Convention justitia.swiss). Nous espérons que la Confédération en fera de même tout prochainement.

Nous sommes favorables à la date d'entrée en vigueur complète de la loi prévue le 1er juillet 2027 telle qu'annoncée lors du séminaire d'informatique juridique à Macolin en avril dernier. En conclusion, le soutien du Conseil d'Etat à l'AP-OCEP est conditionné à l'intégration des observations ci-dessus et des propositions d'adaptation indispensables ci-jointes.

En vous remerciant par avance de l'attention que vous porterez à notre prise de position, nous vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre parfaite considération.

Au nom du Conseil d'Etat

Le président
Christophe Darbellay

CANTON DU VALAIS CONSEIL D'ETAT

La chancelière
Monique Albrecht

Annexe mentionnée
Copie à cornelia.perler@bj.admin.ch

Plateforme de communication électronique dans le domaine judiciaire : consultation sur l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Document d'aide aux autorités cantonales à la prise de position dans le cadre de la consultation

Lors de sa séance du 13 mars 2026, le Conseil fédéral a ouvert la consultation sur l'avant-projet de l'OCEP (AP-OCEP). Les prises de position peuvent être déposées jusqu'au 22 juin 2026.

Le présent d'aide a pour but d'aider les autorités cantonales et les autres milieux intéressés lors de l'élaboration leur prise de position. Il contient pour l'essentiel des explications et des suggestions concernant les différents articles de l'ordonnance ainsi que des propositions de formulation, mais ne constitue pas la prise de position du projet Justitia 4.0.

Auteurs

Autorités cantonales : Alexandra Altherr Müller, Tribunal des assurances sociales/ZH, Patrick Becker, Secrétariat général du Pouvoir judiciaire genevois/GE, Jan Grunder, Tribunal régional Oberland/BE, Stéphane Nakamura, Tribunal de l'arrondissement de la Gruyère/FR, Marc Tille, Service juridique de la sécurité et de la justice/VS, Serge Segura, Tribunal cantonal/VD, Daniel Stehlin, Ministère public/BL, Stephan Walder, Ministère public/ZH, André Zumthurm, Tribunal cantonal/LU

Equipe de projet Justitia 4.0: Jérôme Barraud, Chantal Neuschwander, Christian Renggli, Houri Rousseau

Commentaires, suggestions et propositions de formulation

Préambule

Le projet d'ordonnance omet délibérément de citer les articles qui confèrent au Conseil fédéral la compétence de réglementer le format des documents transmis par voie électronique. Le rapport explicatif précise que, « *pour conserver une vue d'ensemble* », le préambule ne mentionne que les dispositions des lois de procédure qui traitent de la communication en dehors des plateformes de la LPCJ. Même si une référence générale à la LPCJ semble appropriée, il serait préférable de mentionner toutes les normes de délégation contenues dans les lois de procédure. Cela vaut en particulier pour les articles qui confèrent au Conseil fédéral la compétence de définir les formats ; ceux-ci devraient donc logiquement être également mentionnés dans le préambule.

Le préambule devrait dès lors être libellé comme suit :

> *vu la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ),*
> *vu l'art. 6a, al. 2, 21a, al. 2 et 34, al. 1bis de la loi du 20 décembre 1968 sur la procédure administrative du 20 décembre 1968 (PA),*
> *vu l'art. 38e de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF),*
> *vu les art. 128b, al. 3, et 128c, al. 2 et 128e du code de procédure civile du 19 décembre 2008 (CPC),*
> *vu les art. 33a, al. 4, 33b, 33c, al. 2 et 34, al. 3, de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),*
> *vu les art. 76a, al. 2, 103b, al. 3, et 103c, al. 2 et 103e du code de procédure pénale du 5 octobre 2007 (CPP),*
> *vu l'art. 2e de la loi fédérale du 23 décembre 2011 sur la protection extraprocédurale des témoins (Ltém),*
> *vu l'art. 31f de la loi fédérale du 22 mars 1974 sur le droit pénal administratif,*

vu les art. 8c, al. 3, et 8d, al. 2, et 8f de la loi du 23 mars 2007 sur l'aide aux victimes (LAVI),
vu les art. 37d et 38a, al. 2, de la procédure pénale militaire du 23 mars 1979 (PPM),

Chapitre 1 Exploitation et utilisation de plateformes

Section 1 Champ d'application

Art. 1

Selon notre interprétation, l'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral et **ne s'applique donc pas aux cantons**. La valeur ajoutée de l'alinéa 3 n'est pas évidente, étant donné qu'en cas de divergence une loi prévaudrait de toute façon sur la présente ordonnance.

Section 2 Autorisation d'exploiter

Art. 2 Conditions applicables aux plateformes

Les conditions applicables aux plateformes semblent appropriées. Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à l'alinéa 1, lettre c, devrait être fixée dans une annexe à la présente ordonnance ou dans une ordonnance du DFJP.

La fonction de suppression visée à l'alinéa 1, lettre d, est une fonctionnalité qui, le cas échéant, devrait être réglementée dans la section 3 de la présente ordonnance. Par ailleurs, la formulation de cette disposition est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport à la page 11, la fonction de suppression efface l'autorisation individuelle accordée, mais pas le document en tant que tel. Il conviendrait également, s'agissant de la suppression, de faire la distinction entre les autorités et les autres utilisateurs.

Art. 3 Procédure d'autorisation

Pas de remarque.

Section 3 Documents, quittances et apposition d'un cachet

Art. 4 Format des documents

Le présent projet utilise – à l'instar de la LPCJ – le terme « document » plutôt que « fichier » (cf. message LPCJ, p. 20). De notre point de vue, le terme « fichier » est préférable dans l'ordonnance, dans la mesure où il s'agit d'aspects techniques des pièces transmises.

Al. 1

Nous sommes favorables à la définition du format PDF/A pour les documents des autorités et des formats PDF et PDF/A pour les autres participants à la procédure.

Al. 2

Dans de nombreux cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Dans ces cas, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. Si les parties soumettent leurs pièces jointes au format PDF, la conversion par les autorités judiciaires n'est plus nécessaire et toutes les parties disposent du même document. La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si en règle générale les documents sont disponibles au format PDF, cela permet un traitement rapide par les avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers.

Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. De plus, le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées.

Dans certains cas particuliers, le format PDF ne permet pas de restituer suffisamment le contenu informatif d'un document. On peut penser par exemple à des enregistrements audio ou vidéo, à des vidéosurveillances multipistes de tunnels ou à des enregistrements provenant de voitures électriques. Dans ces cas, le DFJP devrait définir quels formats de fichiers peuvent être transmis directement via la plateforme. Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format Zip.

Les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centrale.

L'alinéa 2 devrait donc être libellé comme suit :

> [2] ~~*Les annexes peuvent être remises dans n'importe quel format*~~ *Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine*.

Al. 3 et 4

La sélection proposée de formats de fichiers est adéquate, mais le niveau de norme retenu est critiquable. La définition des formats que les autorités chargées de la procédure doivent traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP.

La liste des formats de documents pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.). Il est nettement plus facile de gérer cela dans une annexe que dans le corps de la présente ordonnance.

Les alinéas 3 et 4 devraient donc être libellés comme suit :

> [3] ~~*L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :*~~*Si l'autorité chargée de la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour qu'elle puisse la transmettre dans un format défini par l'autorité.*
>
> ~~*a. documents écrits : PDF, PDF/A ;*~~
>
> ~~*b. images : BMP, GIF, JPEG, PNG ;*~~
>
> ~~*c. fichiers audio : MP3, OGG, WAV ;*~~
>
> ~~*d. fichiers vidéo : AVI, MOV, MKV, MP4 ;*~~
>
> ~~*e. fichiers d'archives : ZIP, 7z.*~~
>
> [4] ~~*Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée*~~ *Le DFJP définit les formats de fichiers à transmettre via la plateforme*.
>
> [5] ~~*L'autorité qui dirige la procédure fixe un délai approprié.*~~

Art. 5 Quittances

Nous sommes favorables à la réglementation proposée. Il est important que **le nom de la personne responsable d'une autorité**, au sens de l'alinéa 2, lettre b, **ne figure pas** dans la quittance.

Un résultat positif lors du contrôle antivirus visé à l'alinéa 2, lettre d, chiffre 2, constitue un motif possible de rejet par la plateforme, mais pas le seul. La taille ou le format du fichier peuvent également en être la cause. Cette disposition comporte une erreur logique. Les documents non transmis ne peuvent pas figurer sur la **quittance de réception**, puisqu'ils n'ont justement **pas été transmis**. Par conséquent, la quittance ne peut contenir la valeur de hachage de fichiers qui n'ont pas été transmis. Si la plateforme ne parvient pas à transmettre un ou plusieurs documents, l'expéditeur reçoit un message de la plateforme, mais pas de quittance. Le chiffre 2 doit donc être supprimé.

[2] Les quittances comportent en particulier les données suivantes:

a. le type de quittance ;

b. le nom de l'expéditeur, son adresse sur la plateforme et le cas échéant le nom de l'organisation ou de l'entreprise pour laquelle il agit;

c. le nom du destinataire ou de son entreprise et son adresse sur la plateforme;

d. pour la quittance de réception :

1. la liste des documents transmis, leur taille et leur valeur de hachage,

~~*2. laliste des documents qui n'ont pas été transmis en raison du résultat du contrôle antivirus, avec indication de leurtaille,*~~

~~3.~~2. le moment de la transmission à la plateforme;

e. ...

f. ...

g. ...

Les plateformes doivent à l'avenir pouvoir également transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car les fichiers XML, pour des raisons techniques, ne peuvent pas être cachetés.

Art. 6 Apposition d'un cachet par l'autorité expéditrice

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis avant leur envoi à la plateforme ; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement. La plateforme au contraire appose un cachet **après** la transmission à via la plateforme, sur la quittance émise sur la base de l'article 5.

L'article 6 règle **l'apposition d'un cachet sur les documents** par l'autorité dirigeant la procédure **avant leur transmission via une plateforme** (art. 22 al.2 LPCJ). Le projet mentionne que lors que plusieurs documents sont transmis, il suffit qu'un des de ces documents soit muni d'un cachet, ce qui est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examiné indépendamment de la plateforme.

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Par ailleurs l'obligation d'apposer un cachet imposée aux autorités qui dirigent la procédure ainsi qu'aux autorités qui y participent est en contradiction avec le concept technique de la plateforme centralisée.

Pour diverses fonctionnalités de la plateforme, **la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure** est essentielle. Ainsi, seules les autorités qui dirigent la procédure peuvent procéder à des notifications. Seules les adresse de ces autorités qui dirigent la procédure sont visibles pour les tiers dans le répertoire public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités participant à la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations et particuliers et indépendamment d'une procédure (judicaire). Cela ouvrirait la plateforme à toute communication électronique entre autorités, pour laquelle la LPCJ n'offre toutefois pas de base légale suffisante. L'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires.

Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents. L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision ou la décision d'une autorité qui dirige la procédure crée des droits et des obligations. Ceux-ci produisent leurs effets au-delà de la procédure en cause. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète, si le document en question est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités agissent de manière autoritative.

Les autorités participant à la procédure ne peuvent en revanche pas être tenues d'apposer un cachet électronique sur leurs documents. Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent généralement pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante.

Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante pour équiper l'ensemble des autorités suisses d'un cachet électronique. Cela entraînerait pour les cantons un effort organisationnel considérable et des coûts importants.

Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond pas au concept de la LPCJ, laquelle ne prescrit aucune fonctionnalité permettant à la plateforme de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre via la plateforme.

Il serait cependant utile de préciser comment les autorités peuvent signer des documents qui, selon la jurisprudence actuelle, doivent porter la signature de leur auteur, comme les expertises (BSK StPO-Heer, art. 187 N 1). Dans le cas des instituts de médecine légale ou de l'Institut fédéral de métrologie METAS, par exemple, ces expertises peuvent tout à fait être réalisées par des autorités ou, à tout le moins, par des « services administratifs ».

Dans ces cas, l'identité de l'expert qui établit l'expertise est déterminante, raison pour laquelle la signature électronique qualifiée (contrairement au commentaire de l'art. 22 LPCJ dans le message, FF 2023 679ss, p. 30) devrait probablement continuer à s'appliquer à l'avenir.

Il est important de souligner la différence entre l'envoi et consultation en ligne de documents. Comme l'explique à juste titre le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents lors de la consultation en ligne du dossier.

Art. 7 Apposition d'un cachet par la plateforme

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme ; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement (art. 6). La plateforme, en revanche, appose son cachet **après** la transmission sur la plateforme, sur la quittance de réception émise, qui est régie par l'article 5.

Al. 1

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris : le support du cachet électronique de la plateforme est la **quittance, jamais le document transmis.** Dans le cas de la plateforme centralisée, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit :

> *[1] Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

Al. 2

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. **L'alinéa. 2 doit donc être supprimé**.

> *~~[2] Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.~~*

Section 4 Authentification, profils, interfaces et attribution de droits

Art. 8 Authentification des utilisateurs

L'authentification via AGOV conformément à l'alinéa 1 est, de notre point de vue, jugée judicieuse et pertinente.

L'utilisation éventuelle de services d'authentification supplémentaires dans le cadre de futures plateformes cantonales, conformément à l'alinéa 2, est saluée.

À l'avenir, la plupart des autorités seront reliées à la plateforme via une interface. La disposition proposée à l'alinéa 3 laisse une marge de manœuvre suffisante pour mettre en œuvre de futures solutions techniques.

Art. 9 Profils

Al. 2

Cette disposition se réfère uniquement aux autorités chargées de la conduite de la procédure, qui figurent également dans le répertoire d'adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, car une autorité peut disposer de plusieurs sites. La disposition doit être adaptée en conséquence :

[2] Les profils des autorités comprennent au moins les données suivantes :

a. le nom de l'autorité ;

~~b. l'adresse postale ;~~

c. le nom du cachet.

Al. 3, let. a

La reprise de la date de naissance à partir du compte AGOV est particulièrement bienvenue dans le domaine du droit pénal et administratif. Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs doit être considéré comme critique. Il convient donc de renoncer à la collecte des adresses postales des personnes physiques.

[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :

a. pour les personnes physiques : le prénom, le nom, la date de naissance ~~et l'adresse postale~~ ;

Al. 3, let. b

Les entreprises ont des structures variées et des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette dernière n'apporte aucune valeur ajoutée notable dans le cadre de la distribution numérique**. Il convient donc de renoncer à l'adresse postale également pour les organisations.**

L'alinéa devrait donc être formulé comme suit:

[3] Les profils des autres utilisateurs comprennent au moins les données suivantes :

a. pour les personnes physiques : le prénom, le nom, et la date de naissance ~~et l'adresse postale~~ ; ...

b. *pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Al. 4

Le sens de cet alinéa n'est pas compréhensible. Il n'est pas clair s'il s'agit du profil d'une organisation ou d'un particulier. Une clarification par le législateur semble indiquée. Le rapport mentionne la personne responsable d'une organisation. De notre point de vue, il est souhaitable que le rôle de la personne responsable sur la plateforme soit clarifié dans l'ordonnance.

Art. 10 Interface

Cet article permet aux utilisateurs de la plateforme de connecter leurs systèmes à celle-ci via une interface et d'octroyer des droits de représentation à leurs collaborateurs. Cela se fait par l'intermédiaire d'un utilisateur technique qui reçoit un mot de passe numérique (token). La réglementation proposée est donc saluée.

Art. 11 ~~Attribution~~ Confirmation et retrait de droits

La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait de parler de « confirmation » plutôt que d'« attribution ». Nous sommes favorable à la variante proposée à l'alinéa 2.

Section 5 Protection des données, sécurité des données et contrôle antivirus

Art. 12 Durée maximale de conservation des documents et des quittances

Problématique

L'article 12 du projet d'ordonnance OCEP prévoit que les documents et les quittances soient automatiquement supprimées de la plateforme à l'expiration d'un délai de six mois. Nous sommes favorables à la suppression automatique des notifications et des requêtes après un délai raisonnable, car la plateforme est conçue comme une « boîte aux lettres » et non comme un moyen d'archivage à long terme. Ill semble cependant opportun, en ce qui concerne les quittances, de prévoir un délai plus long. Les quittances peuvent encore être nécessaires très tard dans la procédure, par exemple pour prouver le respect d'un délai ou la prise de connaissance d'un document donné. Bien entendu, les autorités doivent veiller à transférer les quittances dans leurs propres logiciels de gestion d'affaires. Cependant, le fait que, en raison du fonctionnement de la plateforme centralisée, elles ne soient pas classées dans les dossiers d'une procédure, par exemple en cas de notifications, peut conduire à ce que le téléchargement des quittances ne soit pas effectué. Contrairement aux requêtes et aux notifications, qui peuvent être renvoyées depuis les systèmes sources, les quittances générées par la plateforme elle-même seraient dans ce cas déjà perdues au bout de six mois. A ce stade-là, une procédure n'est souvent pas encore terminée.

Les quittances peuvent également contenir des données personnelles (telles que les noms des parties à la procédure), ce qui, dans le contexte des procédures judiciaires, peut même en faire des données personnelles particulièrement sensibles. Cependant, ces données, tout comme les pièces du dossier elles-mêmes, bien plus sensibles, sont stockées de manière sécurisée sur la plateforme. À cela s'ajoute le fait que les quittances constituent également de très petites quantités de données qui ne nécessitent pas de stockage supplémentaire important, même si elles restent disponibles longtemps sur la plateforme.

Solution proposée

Pour les raisons exposées ci-dessus, il est proposé ici de modifier ou de compléter l'article 12 AP-OCEP comme suit. Le délai de suppression de trois ans s'aligne sur le délai pendant lequel la Poste suisse permet d'effectuer des recherches dans le courrier. En français le fait que la suppression est automatique manque dans le libellé de l'alinéa 1 et devrait être complété comme suit:

> *Art. 12 Durée maximale de conservation des documents et des quittances*
>
> *[1] Les documents ~~et les quittances~~ enregistrés sur une plateforme sont automatiquement détruits six mois après leur réception ~~ou leur délivrance~~.*
>
> *[2] Lorsque des documents peuvent être consultés, l'autorité qui dirige la procédure fixe le délai pendant lequel ils sont disponibles sur la plateforme. Passé ce délai, ils sont automatiquement supprimés ~~détruits~~.*
>
> *[3] Les quittances sont automatiquement supprimées trois ans après leur délivrance.*

Al. 2

Nous sommes favorable à solution proposée. Il n'est pas nécessaire de prévoir une prolongation du délai dans l'ordonnance, car l'autorité peut ordonner une deuxième consultation du dossier avec les mêmes pièces.

Art. 13 Sécurité des données

La disposition proposée renvoie à la section 3; la mention du chapitre pertinent (2 ?) fait défaut et devrait être ajoutée.

Art. 14 Contrôle antivirus

Du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants.

1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse atteindrait sa limite (espace de stockage, etc.), interromprait l'analyse et le processus d'analyse pourrait prendre tellement de temps que le respect des délais serait compromis en cas de soumission dans l'urgence.

2. Analyse limitée des fichiers volumineux : un fichier qui dépasse la taille maximale fixée est divisé en blocs gérables aux fins de l'analyse de logiciels malveillants, lesquels sont ensuite analysés individuellement. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisatrices et utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :

   - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
   - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analyser pour détecter de logiciels malveillants, car ils sont chiffrés.
   - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
   - En raison des mesures de protection, des fichiers sont rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».

Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail classique, Dropbox...). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et **cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, respectivement avant et après leur transmission via la plateforme**. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus.

Al. 1

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne devrait pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se

trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra fortement du logiciel chargé de la division et de la vérification. Cette limite évoluera également de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels, et devrait pouvoir être facilement adaptée.

L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets à~~ effectuent un contrôle antivirus.*

Al. 2

La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants peut (et devrait) être facilement augmentée par les exploitants de la plateforme en fonction des possibilités techniques et de l'expérience opérationnelle croissante. **L'alinéa 2 doit donc être supprimé.**

> ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~

Al. 3

Pas de remarque.

Al. 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est essentielle selon nous. La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

L'alinéa 4 devrait donc être libellé comme suit :

> [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels.

Al. 5

Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, il ne s'agit manifestement pas d'une quittance, puisqu'aucun document n'a été transmis (voir les commentaires aux art. 5, al. 2, let. d, ch. 2, ci-dessus).

Section 6 Émolument pour l'utilisation de la plateforme centralisée

Le calcul des émoluments se fonde sur les articles 6 et 32 de la LPCJ. Les coûts de la plateforme sont répartis entre les cantons utilisateurs. Pour les membres de la corporation, la part des émoluments est calculée sur la base de la population résidante permanente. Avec les non-membres, la corporation conclut une convention conformément à l'article 6 de la LPCJ. L'indemnisation convenue doit couvrir l'ensemble des frais (y compris les frais d'investissement, FF 2023 679, p. 22) occasionnés par les non-membres. Les coûts pour les non-membres seront donc généralement plus élevés que ceux des membres.

Art. 15 Calcul de l'émolument

Les versions allemande et française ont été comparées et harmonisées ; cela vaut également pour la cohérence terminologique des notions y figurant. Pour plus de clarté, l'alinéa 1 a été scindé en deux (nouveaux) alinéas.

La référence à la planification financière triennale pour la fixation du montant total de l'émolument pour trois ans est saluée. Cette approche fournit une base prévisible et réaliste pour l'émolument fixé annuellement selon la clé de répartition figurant à l'article 16. Au surplus, la mesure corrective prévue à l'alinéa 4 garantit une capacité d'adapter l'émolument si nécessaire.

Le texte suivant est proposé :

> *[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement ~~de~~ de la plateforme centralisée ~~et~~ permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public. ~~Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~.*
>
> *[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.*
>
> *[3]Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.*
>
> *[3~~4~~] Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~il ne couvrent~~ pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.*

Art. 16 Répartition de l'émolument

Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération, mais pas pour les procédures administratives de première instance. La part fédérale de 10 % est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen.

Nous sommes favorables à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixe le montant annuel des émoluments; il tient compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17).

La formulation suivante est proposée :

> *[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :*
>
> *a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;*
>
> *b. tribunaux de la Confédération : 5 % ;*
>
> *c. cantons : 90 %.*
>
> *[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation public proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû; est*

déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.

[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.

Art. 17 Part de l'administration fédérale et du MPC

Aucune remarque.

Art. 18 Part des tribunaux de la Confédération

Aucune remarque.

Art. 19 Échéance

L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du code des obligations s'appliquent par analogie. Il est donc proposé d'adopter le libellé suivant pour cette disposition :

[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.

[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.

[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.

Art. 20 Service comptable cantonal

Aucune remarque.

Art. 21 Évaluation des règles de calcul de l'émolument

Nous sommes favorables à la révision du mode de calcul de l'émolument proposée.

Chapitre 2 Numérisation et renvoi de documents physiques, envoi papier de documents créés par voie électronique

Art. 22 Numérisation de documents physiques

Cette disposition concerne toutes les autorités qui mènent des procédures dont le droit procédural est déclaré applicable par la LPCJ (art. 2 LPCJ). Pour les cantons, ce sont donc le Code de procédure civile, la Loi sur l'aide aux victimes et le Code de procédure pénale qui priment.

Le format PDF/A prescrit à l'alinéa 2 facilite l'archivage des dossiers judiciaires. Il n'est toutefois pas certain que ce format puisse être facilement traité par les applications judiciaires cantonales, qui sont très différentes les unes des autres.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. La résolution de 300 dpi semble judicieuse. Il convient de noter qu'avec une résolution de 300 dpi, la taille du fichier est quatre fois supérieure à celle obtenue avec une résolution de 150 dpi.

Art. 22*a* Renvoi de documents physiques (nouveau)

Problématique

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est indiqué qu'il a été renoncé à intégrer dans l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (AP-OECP) une disposition relative à l'interprétation restrictive de l'article 30 LPCJ, car il n'y avait plus de marge de manœuvre légale à cet effet.

Cette constatation se réfère à l'interprétation de la notion de « documents » contenue dans l'article 30 de la LPCJ, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents. Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas encore dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent tout à fait une marge d'interprétation des dispositions de la LPCJ dans le sens de leur objectif législatif.

En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme « justitia.swiss ». Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur.

Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, une loi visant à introduire les communications judiciaires électroniques instaurera de nouvelles obligations de renvoi dans le processus papier, qui n'existaient pas encore dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur.

Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc très majoritairement jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine.

Même dans le cas, plutôt rare, où des divergences surgiraient a posteriori quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité.

La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ.

L'article 30, alinéa 2, de la LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce.

En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraîne une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur.

Solution proposée

Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2, de la LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il semble nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable.

> [...]***Art. 22a*** *Renvoi des documents physiques*
>
> *Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.*

Art. 22*b* – Notification de copies papier de documents originaux générés par voie électronique (nouveau)

Problématique :

Comment joindre les personnes qui ne sont pas joignables sur la plateforme ?

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est précisé que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k du nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (...) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, du nCPC contient une disposition similaire pour les décisions des tribunaux civils.

L'article 22 concrétise l'article 29 de la LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme. Toutefois, lorsque des particuliers ne souhaitent pas s'inscrire sur une plateforme de transmission électronique, ils conserveront à l'avenir le droit de se voir remettre un exemplaire papier des communications et des décisions.

En particulier, les autorités pénales chargées des contraventions et les services des ordonnances pénales des ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers, parce que, selon l'interprétation (désormais abandonnée) des dispositions procédurales applicables par l'ordonnance relative à la LPCJ, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers pouvant être gérés par voie électronique. C'est notamment dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore.

Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s'agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d'interpréter l'exigence de signature de manière si restrictive qu'elle freine tout progrès.

Il ressort de l'article 22, alinéa 2, LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L'exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l'authentification à l'aide d'un moyen d'identification électronique reconnu ainsi que l'apposition d'un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023 ; FF 2023 679ss, remarques préliminaires concernant l'art. 22, p. 30). Il en résulte que le cachet électronique réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n'y a donc plus de place pour un recours à l'article 14 CO dans le champ d'application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ).

Solution proposée

Il convient certes de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendures lorsqu'elles sont envoyées **sous forme d'original** sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi.

Aujourd'hui déjà, il est d'usage courant auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une **nouvelle obligation est créée dans le monde analogique**. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique. Cela ne peut avoir été l'intention du législateur.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), qui reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier.

La solution proposée présenterait l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier.

Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b:

Art. 22b *Notification de copies papier de documents créés par voie électronique*

Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être

notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.

Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet de l'OCEP, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.

Chapitre 3 Transmission de documents par un autre moyen qu'une plateforme au sens de la LPCJ

Section 1 Recours à d'autres solutions pour la transmission de documents

Art. 23 Exigences

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI). Nous partons du principe que cette disposition vise la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'enquête du ministère public à la police judiciaire ou lors de la transmission des résultats d'actes d'enquête que la police transmet au ministère public.

Un deuxième champ d'application est la chaîne de procédure civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

La transmission physique des dossiers entre les autorités pénales s'effectue actuellement encore souvent par la poste, par courrier interne ou par coursier. La mission confiée à la police pour une mesure d'instruction est généralement formulée par écrit, mais ni la date exacte ni la réception ne sont consignées séparément.

Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faudrait toutefois appliquer d'autres exigences que pour la communication via la plateforme.

La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, nous estimons qu'aucune quittance n'est nécessaire. L'enregistrement dans les logfiles du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 devrait être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.

Art. 24 Transmission par voie électronique entre les autorités

L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils, ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. la consultation relative à l'art. 6 OECP). Une incertitude subsiste à cet égard, notamment en ce qui concerne les corporations de droit public qui n'agissent pas dans l'exercice de la puissance publique.

Cette disposition précise les exceptions prévues à l'article 128c, alinéa 2, CPC, à l'article 103c, alinéa 2, CPP et à l'article 8d, alinéa 2, de la LAVI. Ces exceptions sont justifiées lorsque, dans le cadre de procédures civiles ou pénales, un grand nombre de communications avec les autorités sont nécessaires, communications qui ne font pas partie de la chaîne de procédure pénale ou civile, et lorsque la communication directe, par exemple via une interface, est préférable aux communications électroniques dans le domaine judiciaire via la plateforme, notamment pour la transmission de métadonnées ou pour des raisons de coût. Dans le cadre de la procédure pénale, on peut penser par exemple aux autorités fiscales ou de migration, ou encore aux grandes entreprises de transport ou aux instituts de médecine légale, qui devraient également relever de la notion d'autorité. Il en va de même pour certaines autorités fédérales telles que l'OFDF.

Les conditions devraient s'inspirer de l'article 23 et ne pas aller au-delà. En tout état de cause, on ne voit pas pourquoi l'article 24 prévoit des exigences plus strictes, étant donné que l'article 103c, alinéa 2, CPP – contrairement à l'art. 103b, alinéa 2, CPP, qui prévoit l'enregistrement du moment de transmission et la protection du dossier contre toute modification et toute consultation non autorisée – n'impose aucune exigence quant à la documentation d'une transmission.

Section 2 Transmission de documents par voie électronique dans le domaine de la poursuite pour dettes et la faillite

Art. 25

Aucune remarque.

Section 3 Attestation par voie électronique de l'exactitude du procès-verbal en procédure pénale et en procédure pénale militaire

Art. 26 Aucune remarque.

Chapitre 4 Dispositions finales

Art. 27 Abrogation et modification d'autres actes

Aucune remarque.

Art. 28 Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme sera donc assuré par des émoluments à partir de début 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi afin de permettre la planification financière des cantons à partir de 2028.

Abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures administratives

Aucune remarque.

Abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite

En raison de l'abrogation de l'ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite, IncaMail et PrivaSphere ne pourront plus être utilisés dans les procédures engagées après l'entrée en vigueur de l'ordonnance. Il appartient donc aux cantons de choisir et de mettre à disposition des canaux appropriés pour les procédures administratives qui ne peuvent pas être traitées via la plateforme justitia.swiss.

Art. 14a Signatures et cachets électroniques vérifiés par le validateur

Aucune remarque.

Art. 14b Apposition et validation de signatures et de cachets électroniques

Aucune remarque.

Sicherheitsdirektion, Postfach, 6301 Zug

Nur per E-Mail

Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

T direkt +41 41 594 14 73
martin.meier1@zg.ch
Zug, 18. Juni 2026 zgmear
SD SDS 7.11 / 479

Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)
Stellungnahme des Kantons Zug

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie die Kantonsregierungen eingeladen, sich bis am 22. Juni 2026 vernehmen zu lassen. Der Regierungsrat des Kantons Zug hat die Sicherheitsdirektion mit der direkten Erledigung der Vernehmlassung beauftragt. Gerne nehmen wir zur Vorlage wie folgt Stellung.

I. Allgemeines

Wir begrüssen das Ziel, den elektronischen Rechtsverkehr in Justiz- und Verwaltungsverfahren schweizweit zu vereinheitlichen und die rechtlichen Grundlagen für durchgängig digitale und medienbruchfreie Verfahren zu schaffen. Beim Vorentwurf der VEKJ besteht jedoch noch Klärungs- und Präzisierungsbedarf. Dies betrifft unter anderem die Authentifizierung, die zulässigen Dokumenten- und Datenformate, die Übermittlung grosser und forensischer Datenbestände, die Qualitätssicherung bei der Digitalisierung physischer Unterlagen sowie den Umgang mit strukturierten Daten, KI-bezogenen Verarbeitungsschritten und Transkriptionsformaten.

Teilweise wurden diese Aspekte bereits in der fundierte Arbeitshilfe zur Vernehmlassungsvorlage aufgegriffen, die eine Arbeitsgruppe zusammen mit dem Projektteam von Justitia 4.0 erarbeitet hat (vgl. Beilage 1). Vorliegend ist auf diese Arbeitshilfe zu verweisen, deren Analysen und Schlussfolgerungen grossmehrheitlich geteilt werden. Besonders hervorzuheben ist dabei der Anpassungsbedarf hinsichtlich Art. 2 Abs. 2 Bst. c, Art. 4 Abs. 2, Art. 6, Art. 12 und Art. 22a und 22b VEKJ.

Es sind aus Sicher des Kantons Zug jedoch auch Änderungen im Verordnungstext angezeigt, die über die Vorschläge in der Arbeitshilfe hinausgehen bzw. andere Themenkomplexe betreffen. Im Einzelnen stellen wir daher folgende Anträge und machen folgende Stellungnahmen:

II. Anträge und Stellungnahmen sowie Begründung

1. Art. 3 Abs. 2 und 3 VEKJ seien dahingehend zu ergänzen, dass allgemeine qualitative Komponenten für das Bewilligungsverfahren und die Gesuche in den Verordnungstext aufgenommen werden.

Begründung:
Aufgrund der Bedeutung der Plattformen sollte in Art. 3 Abs. 2 und 3 VEKJ (analog zu Art. 2 Absatz 2 VEKJ) eine allgemeine qualitative Komponente für das Bewilligungsverfahren und die Gesuche mit in den Verordnungstext aufgenommen werden. Etwa, dass die Plattformen unter Anwendung anerkannter Methoden und aktueller Standards entwickelt wurden und zum Zeitpunkt der Gesuchseinreichung dem aktuellen Stand der Technik entsprechen. Auch sollten übliche praktische Prüfungen ausdrücklich möglich sein, um die Angaben aus den Gesuchen zu kontrollieren, insbesondere hinsichtlich der Sicherheit der Systeme (z.B. Durchführung von Pentests).

2. Art. 4 VEKJ sei mit Blick auf die Übermittlung von Beilagen klarer zu formulieren, insbesondere welche Formate als Standardformate für die interoperable Bearbeitung gelten, welche Formate nur ausnahmsweise zulässig sein sollen und wie mit künftigen Formaten umzugehen ist.

Begründung:
Der Vorentwurf erlaubt Beilagen in beliebigen Formaten, während Behörden nur eine beschränkte Liste von Formaten zur Auswahl haben. Diese Regelung kann zu einem erheblichen Spannungsverhältnis zwischen formeller Zulässigkeit und praktischer Verwendbarkeit führen. Es ist absehbar, dass Beilagen zwar rechtlich zulässig eingereicht werden, in der Praxis aber aus technischen, organisatorischen oder sicherheitsbezogenen Gründen nicht geöffnet oder nicht zweckmässig verarbeitet werden können. Dies gilt besonders für polizeiliche und strafprozessuale Konstellationen, in denen nicht nur klassische Dokumente, sondern auch Audio-, Video-, Bild-, Extraktions-, Analyse- und Containerformate übermittelt werden. Vor diesem Hintergrund ist es angezeigt, dass der Verordnungsentwurf klarer regelt, welche Formate als Standardformate für die interoperable Bearbeitung gelten, welche Formate nur ausnahmsweise zulässig sein sollen und wie mit künftigen Formaten umzugehen ist. Dies betrifft insbesondere strukturierte Daten aus Fachanwendungen und Analysesystemen. Dabei ist auch zu klären, ob und unter welchen Voraussetzungen Daten aus myABI und anderen Systemen, insbesondere auch aus Analysesystemen, rechtlich an Plattformen oder weitere Datenplattformen übergeben werden dürfen, in welchem Format dies zu erfolgen hat und wie mit heutigen sowie künftigen

Austauschformaten umzugehen ist. Diese Punkte sind für die Praxis zentral, bleiben im Vorentwurf jedoch zu offen.

3. Es sei zu prüfen, ob der Umgang mit strukturierten Daten, Analyseergebnissen, maschinell erzeugten Auswertungen, KI-gestützten Bearbeitungsschritten und Transkriptionsformaten bereits auf Verordnungsstufe klarer abgebildet werden muss.

Begründung:
Der erläuternde Bericht hält fest, dass strukturierte Daten als Beilage übermittelt werden können, während für Dokumente Siegelungsvorgaben gelten und das EJPD die technischen Vorgaben sowie das Datenformat der Schnittstellen später regeln soll. Damit wird ein wesentlicher Teil der praktischen Umsetzung verschoben. Für die betroffenen Behörden bleibt damit unklar, welche Formate für strukturierte Daten verbindlich sein werden, wie Schnittstellen technisch und rechtlich ausgestaltet werden und wie die Interoperabilität zwischen Plattformen und Fachsystemen konkret sichergestellt werden soll. Vor diesem Hintergrund ist zu prüfen, ob der Umgang mit strukturierten Daten, Analyseergebnissen, maschinell erzeugten Auswertungen, KI-gestützten Bearbeitungsschritten und Transkriptionsformaten bereits auf Verordnungsstufe klarer abgebildet werden muss. Gerade in der polizeilichen und strafprozessualen Praxis gewinnen automatisierte Auswertungen, Transkriptionen von Audio- und Videoinhalten sowie strukturierte Exportformate aus Fach- und Analysesystemen stark an Bedeutung. Es braucht klare Vorgaben, ob solche Inhalte als Beilage, als strukturierter Datensatz oder in anderer Form übermittelt werden dürfen, welche Anforderungen an Integrität, Nachvollziehbarkeit und Lesbarkeit gelten und wie die spätere beweisrechtliche Verwertbarkeit sichergestellt wird.

4. In Art. 5 Abs. 1 VEKJ sei der Begriff «zusammen übermittelt» zu präzisieren, insbesondere in zeitlicher, inhaltlicher und funktioneller Hinsicht.

Begründung:
Es ist klarer zu umschreiben, was «zusammen übermittelt» in zeitlicher, inhaltlicher und funktioneller Hinsicht bedeutet. Es wird aktuell wohl davon ausgegangen, dass es sich um eine zusammenhängende Übermittlung innerhalb eines Übertragungsvorgangs handelt und die übertragenen Dateien nur ein einziges Verfahren betreffen.

5. Mit Blick auf Art. 5 Abs. 2 VEKJ sei zu prüfen, ob bei einer automatisierten Übertragung ein diesbezüglicher Hinweis auf der Quittung aufgeführt werden soll.

Begründung:
Wenn eine Übertragung automatisiert via Schnittstelle vorgenommen wird, sollte auf der Quittung auch ein Hinweis zu finden sein, sofern dies nicht – analog zum Namen der Plattform – im von der Plattform angebrachten Siegel enthalten sein sollte.

6. In Art. 5 Abs. 2 Bst. d Ziff. 1 VEKJ sei der Begriff «Hashwert» zu präzisieren.

Begründung:
Der Begriff «Hashwert» ist nicht ausreichend präzise, um seine Funktion für die Quittungen eindeutig zu definieren. Während in der Verordnung der verwendete Algorithmus nicht an- oder vorgegeben werden sollte, wäre eine begriffliche Präzisierung wünschenswert, um den Zweck der Hashfunktion näher einzugrenzen (z.B. «kryptografischer Hashwert [kryptographischer Fingerabdruck der Datei]»).

7. Art. 5 Abs. 4 VEKJ sei dahingehend zu ergänzen, dass für das maschinenlesbare Format ein standardisiertes Format festzulegen ist.

Begründung:
Wenngleich das maschinenlesbare Format nicht auf Verordnungsstufe definiert werden muss, so sollte doch festgehalten werden, dass auch hierfür ein standardisiertes Format festzulegen und zu nutzen ist.

8. Mit Blick auf Art. 8 VEKJ sei zu prüfen, ob neben AGOV auch andere gleichwertige staatliche oder staatlich anerkannte Authentifizierungsmittel zugelassen werden können.

Begründung:
Der Vorentwurf sieht vor, dass für die Authentifizierung grundsätzlich AGOV verwendet wird. Die schweizerische E-ID dient demgegenüber nur als Identitätsnachweis innerhalb von AGOV. Diese Ausgestaltung erhöht die Systemkomplexität und schafft eine starke Abhängigkeit von einem einzelnen Authentifizierungsdienst. Ein praktischer oder sicherheitstechnischer Mehrwert dieser Doppelstruktur ist nicht ersichtlich.
Vor diesem Hintergrund ist zu prüfen, ob neben AGOV auch andere gleichwertige staatliche oder staatlich anerkannte Authentifizierungsmittel zugelassen werden können, sofern sie ein gleich hohes Sicherheitsniveau gewährleisten. Damit könnte die technische Resilienz erhöht und unnötige Abhängigkeiten vermieden werden.

9. In Art. 8 Abs. 2 VEKJ sei die Formulierung «sie können zusätzliche Dienste» zu verwenden.

Begründung:
Mit Blick auf Art. 8 Abs. 2 VEKJ sei anstelle der Formulierung «sie können einen anderen Dienst» die offenere Formulierung «sie können zusätzliche Dienste» zu bevorzugen.

10. Mit Blick auf Art. 9 Abs. 2 und 3 VEKJ sei zu prüfen, ob eine digitale Kontaktadresse als Mindestangabe aufzunehmen ist.

Begründung:
Es wird davon ausgegangen, dass eine digitale Kontaktadresse für jede Benutzerin und jeden Benutzer (wie E-Mail-Adresse oder Mobilfunknummer) über die Authentifizierungsmethode vorliegt und dadurch automatisch im Profil verfügbar ist. Sollte dies nicht der Fall sein, sollte eine digitale Kontaktadresse auch als Mindestangabe gefordert werden.

11. Art. 11 VEKJ sei dahingehend zu ergänzen, dass ein Entzug auch bei missbräuchlicher Verwendung der Plattformen möglich ist.

Begründung:
Eine Möglichkeit zum Entzug sollte auch bei missbräuchlicher Verwendung der Plattformen vorgesehen werden.

12. In Art. 12 Abs. 2 VEKJ sei zusätzlich zu berücksichtigen, wie eine spätere identische Wiederbereitstellung sichergestellt wird, wie Integrität und Hashwerte dokumentiert werden und wie die Nachvollziehbarkeit bei wiederholter Akteneinsicht gewährleistet bleibt.

Begründung:
Die automatische Löschung von Plattformkopien nach Ablauf der Einsichtsfrist mag datenschutzrechtlich nachvollziehbar sein. Aus Sicht der Praxis bleiben aber wichtige Fragen offen. Dies gilt namentlich für umfangreiche Akten, forensische Daten, extern gespeicherte Bestände oder Inhalte, die nur mit Spezialsoftware sinnvoll genutzt werden können. Nicht geregelt ist, wie eine spätere identische Wiederbereitstellung sichergestellt wird, wie Integrität und Hashwerte dokumentiert werden und wie die Nachvollziehbarkeit bei wiederholter Akteneinsicht gewährleistet bleibt. Gerade bei digitalen Beweismitteln ist dies für die Beweissicherheit wesentlich.

13. Mit Blick auf Art. 14 VEKJ sei zu prüfen, ob klarere Vorgaben für den Umgang mit grossen Dateien, erhöhten Sicherheitsrisiken und alternativen Übermittlungswegen notwendig sind.

Begründung:
Die vorgesehene Virenprüfung überzeugt für kleinere Dateien eher als für grosse Datenbestände. Der Vorentwurf geht selbst davon aus, dass Dateien ab 64 MB nur eingeschränkt geprüft werden können. Werden grössere Dateien segmentiert geprüft oder bloss besonders gekennzeichnet, entsteht in der Praxis ein erhebliches Problem: Solche Dateien werden in sicherheitssensiblen Umgebungen regelmässig gerade nicht geöffnet. Damit droht die Regelung ihren Zweck zu verfehlen. Eine formell zulässige elektronische Übermittlung nützt wenig, wenn die empfangende Behörde die Datei aus

Sicherheitsgründen faktisch nicht verwenden kann. Wir erachten deshalb klarere Vorgaben für den Umgang mit grossen Dateien, erhöhten Sicherheitsrisiken und alternativen Übermittlungswegen als notwendig.

Besonders kritisch ist der Umgang mit forensischen Beweismitteln und grossen Datenbeständen. Der erläuternde Bericht hält ausdrücklich fest, dass forensische Auswertungen beschlagnahmter Geräte Datenmengen im Umfang von hunderten Gigabytes oder gar Terabytes umfassen können und dass hierfür allenfalls besondere Lösungen oder Zugriffe auf forensische Applikationen vorgesehen werden. Zugleich bleibt offen, wie in solchen Fällen die Integrität der Daten, die Unveränderthеit und die Chain of Custody gewahrt werden sollen. Für forensische Datenträgerabbilder, Extraktionen aus Mobiltelefonen, Logdaten, Analysecontainer und vergleichbare digitale Beweismittel gelten hohe Anforderungen an Nachvollziehbarkeit und Unveränderthеit. Das Aufteilen grosser Dateien, die manuelle Sonderbehandlung oder die Übermittlung über nicht forensiktaugliche Systeme stehen dazu in einem klaren Spannungsverhältnis. Die Geeignetheit der BEKJ-Plattformen als Übermittlungsweg für forensische Rohdaten und vergleichbare Beweismittel ist damit nicht ohne Weiteres gegeben. Es ist zu prüfen, ob es für solche Daten gegebenenfalls eine Sonderregelung oder eine separate, Forensik-taugliche Austauschlösung braucht.

14. Mit Blick auf Art. 14 Abs. 1 VEKJ sei zu prüfen, ob der Begriff «Virenprüfung» angepasst werden soll.

Begründung:
Der Begriff «Virenprüfung» ist nicht ausreichend, um alle erforderlichen Sicherheitsmassnahmen beim Entgegennehmen von Dateien zu beschreiben. Er ist zu eng und technisch veraltet konnotiert. Es sollte neutral von «Dateisicherheitsprüfung» gesprochen werden. Dies ist selbst in dem Fall zu empfehlen, wenn die Plattform heute tatsächlich nur eine Virenprüfung durchführen sollte – was jedoch nicht als ausreichend angesehen wird. Vor diesem Hintergrund sollte eine jeweils aktuelle Richtlinie vorliegen, welche Mindestanforderungen an die Dateisicherheitsprüfungen der Plattformen gestellt werden.

15. Mit Blick auf Art. 14 VEKJ sei zu ergänzen, dass die Aufteilung nach Abs. 2 nur temporär für die Dateisicherheitsprüfung erfolgt. Zudem sei mit Blick auf Abs. 3 zu prüfen, ob je nach Konstellation der Empfänger anstelle der Plattformbetreiberin die für den Verzicht relevante Stelle ist.

Begründung:
Es sollte ergänzt werden, dass die Aufteilung nach Art. 14 Abs. 2 VEJK nur temporär für die Dateisicherheitsprüfung erfolgt. Damit wird klargestellt, dass der Empfänger keine aufgeteilten Dokumente erhält. Ferner ist zu prüfen, ob je nach Konstellation der Empfänger (z.B. ein Gericht) anstelle der Plattformbetreiberin die für den Verzicht gemäss Art. 14 Abs. 3 VEKJ relevante Stelle sei.

16. Art. 22 VEKJ sei dahingehend zu ergänzen, dass Mindeststandards für die Digitalisierung, die Qualitätssicherung und den Einsatz entsprechender Systeme formuliert werden.

Begründung:
Die Pflicht zur Digitalisierung physischer Eingaben und zur OCR-Erkennung ist grundsätzlich nachvollziehbar. Der Vorentwurf bleibt bei den Anforderungen an die Qualitätssicherung jedoch zu allgemein. Er verlangt zwar Qualitätskontrolle und OCR, nennt aber keine hinreichend konkreten technischen und organisatorischen Mindeststandards für Scanprozesse, OCR-Werkzeuge, Protokollierung, Qualitätssicherung und Datensicherheit. Es ist fraglich, ob dies bei sensiblen Akten, polizeilichen Unterlagen und beweisrelevanten Dokumenten ausreichend ist. Ohne klare Mindestanforderungen entstehen Risiken für die Lesbarkeit, die Vollständigkeit, die Beweisqualität und den Schutz von Personendaten. Dies gilt umso mehr, wenn künftig OCR- oder Transkriptionsfunktionen ganz oder teilweise KI-gestützt erfolgen. Vor diesem Hintergrund ist eine Präzisierung angezeigt, welche Mindeststandards für die Digitalisierung, die Qualitätssicherung und den Einsatz entsprechender Systeme gelten.

17. Art. 22 VEKJ sei hinsichtlich der Vorgabe einer Farbtiefe sowie der Übereinstimmung mit den physischen Dokumenten zu präzisieren.

Begründung:
Die Vorgabe einer Farbtiefe von 8 Bit gemäss Art. 22 Abs. 1 VEKJ würde das in vielen Fällen ausreichenden Scannen von Texten in schwarz-weiss (1 Bit) verhindern.
Ferner bedeutet der in Art. 22 Abs. 4 VEKJ verwendete Begriff «übereinstimmen» üblicherweise eine vollständige Übereinstimmung, also eine jederzeitig hundertprozentige Scanqualität und OCR-Erkennungsrate. Im erläuternden Bericht wird jedoch von einem «Best Effort» gesprochen. Es ist fraglich, ob dies begrifflich vereinbar ist.

18. Mit Blick auf Art. 22 VEKJ sei zu prüfen, wie mit nicht oder nur beschränkt digitalisierbaren Beweismitteln umzugehen ist.

Begründung:
Grundsätzlich wird die in der Arbeitshilfe vorgeschlagene Änderung der Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten (Kapitel 2 der Arbeitshilfe) begrüsst (Art. 22-22b VEKJ). Der bisherige Vorentwurf führt nämlich im Ergebnis dazu, dass physisch eingereichte Akten digitalisiert und anschliessend zurückgesendet werden müssen. Das ist systemisch aufwendig und schafft problematische Anreize. Gleichzeitig bleibt im Vorentwurf offen, wie mit nicht oder nur beschränkt digitalisierbaren Beweismitteln umzugehen ist, etwa mit Gegenständen, Spurenträgern oder anderen originär physischen Beweismitteln. Vor diesem

Hintergrund ist unter Umständen noch klarer zwischen digitalisierbaren Unterlagen und physischen Beweismitteln zu unterscheiden.

19. Art. 26 VEKJ sei hinsichtlich der Formulierung zur Unveränderlichkeit elektronischer Protokolle zu präzisieren.

Begründung:
Die Formulierung zur Unveränderlichkeit elektronischer Protokolle ist aus technischer Sicht nicht präzise. Nicht das Gerät als solches gewährleistet die Unveränderlichkeit, sondern die technische Ausgestaltung des Dokuments oder Datensatzes, insbesondere durch geeignete Signatur-, Siegel- und Integritätsmechanismen. Wir regen deshalb an, den Verordnungstext oder zumindest den erläuternden Bericht entsprechend zu präzisieren, damit keine Missverständnisse über die eigentliche Schutzwirkung und die technischen Anforderungen an elektronische Protokolle entstehen.

III. Schlussbemerkungen

Abschliessend ist festzuhalten, dass wir die Zielsetzung des Vorentwurfs unterstützen. Wie dargelegt besteht in mehreren praxisrelevanten Punkten jedoch Überarbeitungs- bzw. Präzisierungsbedarf. Besonders kritisch zu beurteilen sind die unklare Regelung der zulässigen und künftig zulässigen Daten- und Austauschformate, den Umgang mit strukturierten Daten aus Fach- und Analysesystemen, die fehlende Einordnung von KI-bezogenen Verarbeitungsschritten und Transkriptionsformaten, die unzureichende Regelung für grosse forensische Datenbestände, die begrenzte Praxistauglichkeit der Virenprüfung sowie die fehlenden Mindeststandards für Digitalisierung, OCR und Qualitätssicherung.

Aus diesen Gründen erachten wir eine Überarbeitung des Vorentwurfs vor der Inkraftsetzung als angezeigt.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anträge.

Freundliche Grüsse
Sicherheitsdirektion



Laura Dittli
Regierungsrätin

Beilage:
Arbeitshilfe zur Vorbereitung der Stellungnahme für kantonale Behörden vom 22. April 2026

Versand per E-Mail an:
- Eidgenössisches Justiz- und Polizeidepartement EJPD (cornelia.perler@bj.admin.ch; als PDF- und Word-Version)
- Finanzdirektion (info.fd@zg.ch)
- Volkswirtschaftsdirektion (info.vds@zg.ch)
- Obergericht (info.og@zg.ch)
- Verwaltungsgericht (info.vg@zg.ch)
- Datenschutzstelle (datenschutz.zug@zg.ch)
- Zuger Polizei (kommandooffice.polizei@zg.ch; Rechtsdienst.Polizei@zg.ch)
- Amt für Justizvollzug (strafanstalt@zg.ch)
- Staatskanzlei (info.staatskanzlei@zg.ch; Abschluss der GEVER-Aufgabe)

Vernehmlassung: Vorentwurf zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VE-VEKJ)

Arbeitshilfe zur Vorbereitung der Stellungnahme für kantonale Behörden

An seiner Sitzung vom 13. März 2026 hat der Bundesrat die Vernehmlassung zum Vorentwurf der VEKJ (VE-VEKJ) eröffnet. Eine Stellungnahme kann bis am 22. Juni 2026 eingereicht werden.

Die vorliegende Arbeitshilfe dient der Unterstützung der kantonalen Behörden und weiteren interessierten Kreise zur Erarbeitung ihrer Stellungnahme. Sie beinhaltet im Wesentlichen Erläuterungen und Anregungen zu den einzelnen Verordnungsartikeln sowie Formulierungsvorschläge, stellt jedoch nicht die Stellungnahme des Projektes Justitia 4.0 dar.

Autorinnen und Autoren

Kantonale Behörden: Alexandra Altherr Müller, Sozialversicherungsgericht ZH, Patrick Becker, Justizleitung GE, Jan Grunder, Regionalgericht Oberland BE, Stéphane Nakamura, Bezirksgericht Greyerz FR, Marc Tille, Rechtsdienst für Sicherheit und Justiz VS, Serge Segura, Kantonsgericht VD, Daniel Stehlin, Staatsanwaltschaft BL, Stephan Walder, Oberstaatsanwaltschaft ZH, André Zumthurm, Kantonsgericht LU

Projektteam Justitia 4.0: Jérôme Barraud, Chantal Neuschwander, Christian Renggli, Houri Rousseau

Erläuterungen, Anregungen und Formulierungsvorschläge

Ingress

Im Vorentwurf fehlen bewusst die Artikel, die dem Bundesrat die Kompetenz zur Regelung des Formats der elektronisch übermittelten Dokumente übertragen. Im erläuternden Bericht wird präzisiert, dass, "um die Übersichtlichkeit zu bewahren", im Ingress lediglich die Bestimmungen der Verfahrensgesetze erwähnt werden, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben. Auch wenn ein allgemeiner Verweis auf das BEKJ angemessen erscheint, wäre es vorzuziehen, alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen. Dies gilt insbesondere für die Artikel, die dem Bundesrat die Kompetenz zur Festlegung der Formate übertragen; diese sollten daher logischerweise ebenfalls im Ingress erwähnt werden.

Der Ingress sollte daher wie folgt ergänzt werden:

> *Der Schweizerische Bundesrat,*
>
> *gestützt auf das Bundesgesetz vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ),*
>
> *die Artikel 6a Absatz 2, 21a Absatz 2 und 34 Absatz 1bis des Verwaltungsverfahrensgesetzes vom 20.Dezember 1968 (VwVG),*
>
> *Artikel 38e des Bundesgerichtsgesetzes vom 17. Juni 2005 (BGG),*
>
> *die Artikel 128b Absatz 3, 128c Absatz 2 und 128e der Zivilprozessordnung (ZPO),*
>
> *die Artikel 33a Absatz 4, 33b, 33c Absatz 2 und 34 Absatz 3 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG),*
>
> *die Artikel 76a Absatz 2, 103b Absatz 3, 103c Absatz 2 und 103e der Strafprozessordnung (StPO),*
>
> *Artikel 2e des Bundesgesetzes vom 23. Dezember 2011 über den ausserprozessualen Zeugenschutz (ZeugSG),*
>
> *Artikel 31f des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR),*
>
> *die Artikel 8c Absatz 3, 8d Absatz 2 und 8f des Opferhilfegesetzes vom 23. März 2007 (OHG)*

und die Artikel 37d und 38a Absatz 2 des Militärstrafprozesses vom 23. März 1979 (MStP), verordnet:

1. Kapitel: Betrieb und Nutzung von Plattformen

1. Abschnitt: Geltungsbereich

Art. 1

Absatz 2 betrifft ausschliesslich bundesrechtliche Verfahren nach VwVG und ist **daher für die Kantone nicht relevant**. Unklar scheint der Mehrwert von **Absatz 3**, gehen Gesetze dieser Verordnung doch ohnehin vor.

2. Abschnitt: Betriebsbewilligung

Art. 2 Anforderungen an die Plattformen

Die Anforderungen an die Plattformen scheinen sachgerecht. Aufgrund der schnellen technischen Entwicklung sollte die maximale Dateigrösse gemäss **Absatz 1 Buchstabe c** jedoch in einem Anhang zur vorliegenden Verordnung oder in einer Departementsverordnung des EJPD festgelegt werden.

Die **Löschfunktion in Absatz 1 Buchstabe d ist eine Funktionalität**, welche – wenn überhaupt - im 3. Abschnitt dieser Verordnung geregelt werden sollte. Zudem ist der Wortlaut der Bestimmung zu absolut formuliert und kaum umsetzbar. Wie der erläuternde Bericht auf Seite 11 zurecht ausführt, wird durch die Löschfunktion die erteilte individuelle Berechtigung gelöscht, nicht jedoch das Dokument als solches. Zudem wäre bei der Löschung zwischen den Behörden und anderen Nutzern zu unterschieden.

Art. 3 Bewilligungsverfahren

Keine Bemerkungen.

3. Abschnitt: Dokumente, Quittungen und Siegelung

Art. 4 Format der Dokumente

Der Vorentwurf verwendet – wie das BEKJ – den Begriff "Dokument" anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: "Der Begriff "Datei" ist für das Gesetz zu technisch."

In diesem Sinne ist in der Verordnung der Begriff Datei – an Stelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

Abs. 1

Die Festlegung des Formats PDF/A für Dokumente von Behörden und der Formate PDF und PDF/A für die übrigen Verfahrensbeteiligten wird begrüsst.

Abs. 2

In vielen Fällen kann der Informationsgehalt eines Dokuments im Format PDF rechtsgenüglich wiedergegeben werden. Insofern soll die Beilage in diesem weit verbreiteten Format eingereicht werden, was die Fallbearbeitung durch die Anwältinnen und Anwälte, die Staatsanwaltschaften, die Gerichte, die Verwaltungsbehörden und durch die weiteren Verfahrensbeteiligten erleichtert. Reichen die Verfahrensbeteiligte ihre Beilagen im Format PDF ein, entfällt die Konversion durch die Justizbehörden, allen Beteiligten liegt das gleiche Dokument vor. Die Digitalisierung soll die Verfahren beschleunigen und die Aktenführung vereinfachen. Wenn Dokumente im Regelfall als PDF-Dokument vorliegen, ermöglicht dies eine speditive Bearbeitung durch die Anwaltschaft und die Behörden. Geschäftsverwaltungssysteme der Anwältinnen, Anwälte und Behörden können aus Sicherheitsgründen nur mit einer beschränkten Anzahl an Dateitypen umgehen ('Whitelistening' von Fileformaten). Wenn das Format der Beilagen frei gewählt werden könnte,

würde dies die Fallbearbeitung erheblich erschweren. Alle Verfahrensbeteiligten müssten zuerst nach dem passenden Programm suchen, um eine Datei zu öffnen. Zudem würde die uneingeschränkte Formatwahl ein erhebliches IT-Sicherheitsrisiko für alle Beteiligten darstellen.

In Einzelfällen kann das Format PDF den Informationsgehalt eines Dokuments nicht genügend wiedergeben. Zu denken ist beispielsweise an Audio- oder Videoaufnahmen, an mehrspurige Tunnelüberwachungen oder Aufzeichnungen aus Elektroautos. Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattformen übermittelt werden können. Aus Sicherheitsgründen scannt die zentrale Plattform alle Dateien auf Viren. Dabei kann die zentrale Plattform grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Für Dokumente, welche nicht direkt über die Plattformen übermittelt werden dürfen, besteht die Möglichkeit zur Übermittlung in einem Container, beispielsweise als Zip-Format.

Welche Dateiformate die Plattformen verarbeiten müssen, ist durch das EJPD nach Anhörung der Betreiberin der zentralen Plattform in einer Departementsverordnung zu regeln.

Absatz 2 sollte daher wie folgt lauten:

> [2] ~~*Die Beilagen können in jedem Format übermittelt werden.*~~ *Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden.*

Abs. 3 und 4

Die vorgeschlagene Auswahl der Dateiformate wird begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen.

Die Liste der unterstützten Dateiformate ist einem stetigen Wandel unterworfen. Es sind daher häufige Anpassungen zu erwarten. Zudem ist das reine Benennen von Formaten in der Verordnung nicht hinreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei dennoch verschlüsselten oder passwortgeschützten Elementen (z.B. Makros in einer Microsoft Excel-Datei, ZIP-Dateien mit teilweise verschlüsselten Dateien etc.). Dies ist in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung.

Absätze 3 und 4 sollten daher wie folgt lauten:

> [3] ~~*Die verfahrensleitende Behörde muss folgende Formate bearbeiten können:*~~
>
> ~~*a. schriftliche Unterlagen: PDF, PDF/A;*~~
>
> ~~*b. Bilddateien: BMP, GIF, JPEG, PNG;*~~
>
> ~~*c. Audiodateien: MP3, OGG, WAV;*~~
>
> ~~*d. Videodateien: AVI, MOV, MKV, MP4;*~~
>
> ~~*e. Archivdateien: ZIP, 7z.*~~
>
> *Kann die verfahrensleitende Behörde eine Beilage im Format, in dem sie eingereicht wurde, nicht öffnen, so räumt sie der einreichenden Partei eine angemessene Frist ein, damit diese die Beilage in einem von der Behörde festgelegten Format einreichen kann.*
>
> [4] ~~*Wird eine Beilage in einem anderen Format eingereicht und kann die verfahrensleitende Behörde die Beilage nicht zweckmässig bearbeiten, so fordert sie die einreichende Person oder Behörde auf, die Beilage in einem von der verfahrensleitenden Behörde festgelegten Format einzureichen oder den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen.*~~ *Das EJPD regelt die über die Plattformen zu übertragenden Dateiformate.*
>
> [5] ~~*Sie räumt ihr eine angemessene Frist ein.*~~

Art. 5 Quittungen

Die vorgeschlagene Regelung wird begrüsst. Es ist wichtig, dass der **Name der verantwortlichen Person einer Behörde** gemäss Absatz 2 Buchstabe b in der Quittung **nicht** aufgeführt wird. Nur der Name der Behörde sollte auf der Quittung erscheinen.

Absatz 2 Buchstabe d konkretisiert die Eingangsquittung und gibt unter anderem vor, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung aufzulisten sind. Mögliche Gründe für eine Rückweisung durch die Plattform sind ein positives Resultat bei der Virenprüfung, die Dateigrösse oder ein Dateiformat, welches die Plattform nicht erkennt.

Absatz 2 Buchstabe d Ziffer 2 präzisiert, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung auszuweisen bzw. aufzulisten sind. Die Bestimmung enthält einen logischen Fehler: Nicht übermittelte Dokumente können auf der **Eingangsquittung** nicht aufgeführt werden, da diese eben **nicht übermittelt** wurden. Die Quittung kann keine Hashwerte von Dateien enthalten, welche nicht übermittelt worden sind. Kann die Plattform ein oder mehrere Dokumente nicht übermitteln, so erhält die Absenderin oder der Absender eine Mitteilung der Plattform, jedoch keine Quittung. Die Ziffer 2 ist daher zu streichen:

[2] Die Quittungen müssen insbesondere folgende Angaben enthalten:

a. die Art der Quittung;

b. den Namen der Absenderin oder des Absenders, ihre oder seine Adresse auf der Plattform und gegebenenfalls den Namen oder die Firma der Organisation, für welche die Absenderin oder der Absender handelt;

c. den Namen oder die Firma der Adressatin oder des Adressaten sowie ihre oder seine Adresse auf der Plattform;

d. bei einer Eingangsquittung:

1. die Liste der übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte,

~~2. die Liste der aufgrund des Resultats der Virenprüfung nicht übermittelten Dokumente und deren Grösse,~~

~~3.~~2. den Zeitpunkt der Übermittlung an die Plattform;

e. bei einer Abrufquittung: den Zeitpunkt des erstmaligen Abrufs;

f. bei einer Nichtabholquittung: den Zeitpunkt der Übermittlung an die Plattform;

g. beim Versand oder erstmaligen Abruf aufgrund der Weitergabe einer Berechtigung: den Namen der Person, in deren Name der Versand oder Abruf erfolgt.

Die Plattformen müssen künftig auch strukturierte Daten übermitteln können, beispielsweise in Form von XML-Dateien. Die Ausnahmen in den Absätzen 4 und 5 sind daher wesentlich, da XML-Dateien aus technischen Gründen nicht gesiegelt werden können.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Im elektronischen Rechtsverkehr wird das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben. Die Plattform dagegen bringt ihr Siegel **nach** der Übermittlung auf die Plattform auf der ausgestellten Eingangsquittung gestützt auf Artikel 5 an.

Artikel 6 regelt die **Sieglung der Dokumente** durch die verfahrensleitende Behörde **vor der Übermittlung über eine Plattform** (Art. 22 Abs. 2 BEKJ). Der Vorentwurf führt aus, dass bei der Übermittlung von mehreren Dokumenten die Sieglung eines Dokuments genüge. Dies ist korrekt. Zu ergänzen ist, dass die Siegelung durch die verfahrensleitende Behörde unabhängig von der Anzahl der übermittelten Dokumente erfolgt. Auch ein einzelnes Dokument, welches die verfahrensleitende Behörde übermittelt, muss gesiegelt werden, damit die Authentizität des Dokuments unabhängig von einer Plattform überprüft werden kann.

Die Ausführungen im erläuternden Bericht, wonach eine Behörde alle Dokumente mit einem Siegel versehen muss, widersprechen dem Wortlaut der Verordnung: Die Siegelung eines Dokuments durch die verfahrensleitende Behörde genügt. Zudem entspricht die Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden nicht dem technischen Konzept der zentralen Plattform.

Die **Unterscheidung zwischen verfahrensleitenden und verfahrensbeteiligten Behörden** ist für verschiedene Funktionalitäten der zentralen Plattform essenziell. Beispielsweise können nur verfahrensleitende Behörden Zustellungen vornehmen. Nur die Adresse von verfahrensleitenden Behörden ist für Drittpersonen aus dem öffentlichen Verzeichnis der zentralen Plattform ersichtlich. Würde an der Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden festgehalten, könnten alle Behörden uneingeschränkt und verfahrensunabhängig Zustellungen an andere Behörden, Organisationen und Privatpersonen vornehmen. Dies würde die zentrale Plattform für jegliche elektronische Kommunikation zwischen Behörden öffnen, wofür das BEKJ jedoch keine hinreichende gesetzliche Grundlage liefert. Sinn und Zweck des BEKJ ist es, die elektronische Kommunikation in Justizverfahren zu ermöglichen.

Nur verfahrensleitende Behörden sind verpflichtet, ihre Dokumente elektronisch zu siegeln. Artikel 22 Absatz 2 BEKJ ist daher einschränkend auszulegen. Das elektronische Siegel stellt die Herkunft, den Zeitpunkt, die Integrität und die Authentizität des gesiegelten Dokuments sicher. Die Verfügung oder der Entscheid einer verfahrensleitenden Behörde begründen Rechte und Pflichten und entfalten Wirkung über das einzelne Verfahren hinaus. Betroffene müssen daher unabhängig von einem konkreten Verfahren oder von der zentralen Plattform prüfen können, ob das fragliche Dokument integer und authentisch ist und von der dafür zuständigen Behörde erstellt wurde. Das elektronische Siegel ist zusammengefasst genau dort notwendig, wo Behörden autoritativ auftreten.

Verfahrensbeteiligte Behörden dagegen dürfen nicht verpflichtet werden, ihre Dokumente zu siegeln. Die Dokumente, welche verfahrensbeteiligte Behörden in einem Justizverfahren übermitteln, begründen in der Regel keine neuen Rechte und Pflichten. Typischerweise handelt es sich bei diesen Dokumenten um Auszüge aus bestehenden Registern, Auszüge aus bestehenden Akten früherer Verfahren, bereits eröffnete Verfügung oder Entscheide aus abgeschlossenen Verfahren, welche nun für ein Justizverfahren zur Verfügung gestellt werden. Die Authentifizierung auf der zentralen Plattform ermöglicht die korrekte Identifikation der Behörde. Will ein Verfahrensbeteiligter die Integrität oder Authentizität eines von einer verfahrensbeteiligten Behörde übermittelten Dokuments in Frage stellen, ist dies eine Frage der Beweiswürdigung im entsprechenden Verfahren.

Würde an der Siegelpflicht für alle Behörden gemäss erläuterndem Bericht festgehalten, so müssten alle Schweizer Behörden auf allen Stufen mit einem Siegel ausgestattet werden. Für die flächendeckende Ausstattung aller Schweizer Behörden mit einem elektronischen Siegel liefert das BEKJ keine genügende gesetzliche Grundlage. Für die Kantone wäre zudem eine flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden.

Gemäss erläuterndem Bericht müssen Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, nicht mehr gesiegelt werden. Diese Aussage entspricht nicht dem Konzept des BEKJ. Das BEKJ schreibt keine Funktionalität vor, wonach die zentrale Plattform qualifizierte elektronische Signaturen von Behördenmitgliedern einer Behörde zuordnet. Aus diesem Grund müssen verfahrensleitende Behörden Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, vor dem Versand über die Plattform standardmässig mit ihrem Siegel versehen.

Es müsste hingegen geklärt werden, wie Behörden Dokumente unterzeichnen können, die gemäss gegenwärtiger Rechtsprechung eine Unterschrift der Autorenschaft tragen müssen, so etwa Sachverständi-

gengutachten (BSK StPO-Heer, Art. 187 N 1). Diese können etwa im Fall von rechtsmedizinischen Instituten oder im Fall des Eidgenössischen Instituts für Metrologie METAS durchaus auch von Behörden oder zumindest von "Amtsstellen" erbracht werden. In diesen Fällen ist es erheblich, welche sachverständige Person das Gutachten erstattet, weshalb die qualifizierte elektronische Signatur (entgegen der Kommentierung zu Art. 22 BEKJ in der Botschaft, BBl 2023 679, S. 30), möglicherweise auch inskünftig noch zur Anwendung gelangen müsste.

Wichtig zu ergänzen ist die Unterscheidung zwischen Versand und Akteneinsicht. Bei der Akteneinsicht besteht, wie der erläuternde Bericht zu Artikel 7 ausführt, dagegen keine Pflicht zur Siegelung der Dokumente durch die verfahrensleitende Behörde.

Art. 7 Siegelung der Dokumente durch die Plattformen

Im elektronischen Rechtsverkehr soll das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt werden. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben (Art. 6). Artikel 7 bezieht sich dagegen auf die Siegelung der Quittung **nach** der Übermittlung durch die zentrale Plattform.

Abs. 1

Der Grundsatz der Siegelung durch die Plattformen wird im Vorentwurf korrekt wiedergegeben: Träger des Siegels der Plattform ist die **Quittung, nie das übermittelte Dokument.** Im Falle der zentralen Plattform handelt es sich dabei um die sogenannte Eingangs- oder Abrufquittung. Die zentrale Plattform siegelt die Quittungen der Benutzerinnen und Benutzer, unabhängig davon, ob sie ein oder mehrere Dokumente übermitteln. Absatz 1 sollte daher wie folgt lauten:

> [1] *Werden ~~mehrere~~ Dokumente ~~zusammen~~ übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an. Das Dokument muss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.*

Abs. 2

Absatz 1 beschreibt die Siegelung der Quittungen. Die Übermittlung von gesiegelten Dokumenten folgt den gleichen Regeln wie in Absatz 1. **Absatz 2 muss daher gestrichen werden**.

> *~~[2] Dokumente, die bereits über ein Siegel oder eine qualifizierte elektronische Signatur mit einem Zeitstempel verfügen, müssen nicht erneut mit einem Siegel versehen werden.~~*

4. Abschnitt: Authentifizierung, Profile, Schnittstellen und Berechtigungen

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Die Authentifizierung über AGOV gemäss Absatz 1 ist sinnvoll und zielführend. Die detaillierten Anforderungen sollten in einer Departementsverordnung des EJPD geregelt werden.

Der mögliche Einsatz von zusätzlichen Authentifizierungsdiensten bei künftigen kantonalen Plattformen gemäss Absatz 2 wird begrüsst.

Künftig sind die meisten Behörden über eine Schnittstelle mit der zentralen Plattform verbunden. Absatz 3 lässt genügend Spielraum, um künftige technische Lösungen umzusetzen.

Art. 9 Profile

Abs. 2

Diese Bestimmung bezieht sich einzig auf verfahrensleitende Behörden, die auch im Adressverzeichnis der zentralen Plattform erscheinen. Bei verfahrensleitenden Behörden ist auf die Angabe einer postalischen Adresse zu verzichten, da eine Behörde über mehrere Standorte und verschiedene Postadressen verfügen kann. Die Bestimmung ist entsprechend anzupassen.

[2] *Die Profile von Behörden müssen mindestens folgende Angaben enthalten:*

a. Name der Behörde;

~~b. Postadresse;~~

~~c~~ b. Bezeichnung ihres Siegels.

Abs. 3 Bst. a

Die Übernahme des Geburtsdatums aus dem AGOV-Account wird insbesondere im Bereich Straf- und Verwaltungsrecht begrüsst. Zu betonen ist, dass die Privatadresse im AGOV-Account nicht aktualisiert wird. Die Richtigkeit der Privatadresse beruht auf der Selbstdeklaration der Nutzerin oder des Nutzers. Sie wird anlässlich der Identifikation nicht geprüft, weshalb sie nicht verlässlich ist. Auch aus Sicht des Datenschutzes ist die Speicherung der Privatadresse in den Benutzerprofilen als kritisch zu betrachten. In den Profilen der natürlichen Personen sollte daher auf die Erhebung von Postadressen **verzichtet werden**.

Abs. 3 Bst. b

Unternehmen haben verschiedene Strukturen und verschiedene Niederlassungen, weshalb das verwendete digitale Profil nicht mit der Postadresse übereinstimmen muss. Die Postadresse bringt beim digitalen Zustellen daher keinen nennenswerten Mehrwert. **Auch bei Organisationen soll daher auf die Postadresse verzichtet werden.**

Absatz 3 sollte daher wie folgt lauten:

[3] *Die Profile der übrigen Benutzerinnen und Benutzer müssen mindestens folgende Angaben enthalten:*

a. bei natürlichen Personen: Vorname, Name, Geburtsdatum ~~sowie Postadresse~~;

b. bei Organisationen: Name oder Firma ~~und Postadresse~~.

Abs. 4

Der Sinn von Absatz 4 ist nicht verständlich. Es ist unklar, ob sich die Pflicht zur elektronischen Übermittlung auf die natürliche Person oder die Organisation, für welche die natürliche Person tätig ist, Bezug nimmt. Letzteres dürfte der Fall sein. Die Formulierung von Absatz 4 ist dementsprechend zu präzisieren.

Im erläuternden Bericht wird die verantwortliche Person einer Organisation erwähnt. Es ist wünschenswert, dass die Rolle der verantwortlichen Person in Bezug auf die zentrale Plattform in der Verordnung geklärt wird.

Art. 10 Schnittstelle

Dieser Artikel erlaubt den Nutzenden der Plattformen, ihre Systeme via eine Schnittstelle mit der Plattform zu verbinden und ihre Mitarbeitenden mit Vertretungsrechten auszustatten. Dies geschieht über einen technischen Benutzer, der ein digitales Passwort (Token) erhält. Die vorgeschlagene Regelung wird daher begrüsst.

Art. 11 Bestätigung und Entzug der Berechtigungen

Die vorgeschlagene Regelung in Absatz 1 wird begrüsst. Jedoch sollte in der französischen Version wohl eher von *Confirmation* als von *Attribution* gesprochen werden.

Die vorgeschlagenen Variante in Absatz 2 wird begrüsst.

5. Abschnitt: Datenschutz, Datensicherheit und Virenprüfung

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Problemstellung

Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein «Briefkasten» und keine Langzeitablage sein soll. Bei den Quittungen scheint es dagegen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Natürlich müssen die Behörden darum besorgt sein, die Quittungen in ihre eigenen Geschäftsverwaltungen zu überführen. Es kann jedoch aufgrund der Funktionsweise der zentralen Plattform – etwa im Fall von Zustellungen – dazu kommen, dass das Herunterladen der Quittungen unterbleibt. Anders als bei Eingaben und Zustellungen, die aus den Quellsystemen mehrmals erfolgen können, wären die von der Plattform selbst generierten Quittungen bereits nach sechs Monaten irreversibel vernichtet. Zu diesem Zeitpunkt ist ein Verfahren oftmals noch nicht abgeschlossen.

Quittungen können Personendaten enthalten (so etwa die Namen von Verfahrensbeteiligten), was diese im Kontext von Justizverfahren unter Umständen zu besonders schützenswerten Personendaten macht. Jedoch sind diese Daten, wie auch die weitaus sensibleren Aktenstücke selbst, auf der Plattform verschlüsselt gespeichert. Hinzu kommt, dass es sich bei Quittungen um sehr kleine Datenmengen handelt, die keinen hohen zusätzlichen Speicherbedarf verursachen, selbst wenn sie lange auf der Plattform verfügbar bleiben müssen.

Lösungsansatz

In Anlehnung an die Zeitspanne von drei Jahren, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind, wird vorgeschlagen, Artikel 12 wie folgt zu ändern, respektive zu ergänzen:

> *Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen*
>
> *[1] Die auf einer Plattform gespeicherten Dokumente ~~und Quittungen~~ werden sechs Monate nach der Entgegennahme ~~beziehungsweise nach der Erstellung~~ automatisch vernichtet.*
>
> *[2] Stehen Dokumente zur Akteneinsicht zur Verfügung, so bestimmt die verfahrensleitende Behörde, wie lange die Dokumente auf der Plattform abrufbar sind. Nach Ablauf der Frist werden die Dokumente automatisch ~~vernichtet~~ gelöscht.*
>
> *[3] Quittungen werden drei Jahre nach ihrer Erstellung automatisch gelöscht.*

Abs. 2

Die vorgeschlagene Lösung wird begrüsst. Eine Verlängerung der Frist muss in der Verordnung nicht vorgesehen werden, da die Behörde eine zweite Akteneinsicht mit denselben Akten anordnen kann.

Art. 13 Datensicherheit

Die vorgeschlagene Bestimmung verweist auf den 3. Abschnitt, die Angabe des relevanten Kapitels (2.?) fehlt und sollte ergänzt werden.

Art. 14 Virenprüfung

Bei der vorgesehenen Prüfung auf Schadsoftware sind aus technischer Sicht drei Fälle zu unterscheiden:

1. Vollständige Prüfung der übermittelten Dateien: Die Maximalgrösse der einzelnen Dateien darf eine festgelegte Obergrenze nicht überschreiten, da die Prüfsoftware sonst ihr Limit (Speicherplatz usw.) erreichen, die Prüfung abbrechen und der Prüfvorgang so viel Zeit in Anspruch nehmen könnte, dass die Einhaltung von Fristen, besonders bei einer zeitlich knappen Eingabe, gefährdet wäre.

2. Eingeschränkte Prüfung grosser Dateien: Eine Datei, welche die festgelegte Obergrenze überschreitet, wird zum Zweck der Schadsoftware-Prüfung in handhabbare Blöcke zerlegt, die dann einzeln auf Schadsoftware geprüft werden. Dieses Verfahren ist jedoch weniger zuverlässig als die vollständige Prüfung der übermittelten Dateien. Schadsoftware, die durch die Aufteilung in prüfbare Blöcke auf zwei aufeinanderfolgende Blöcke verteilt wird, wird unter Umständen nicht mehr als Schadsoftware erkannt. Dies muss den Nutzerinnen und Nutzern der Plattform verständlich angezeigt werden. Insbesondere ist dem Empfänger klar zu signalisieren, dass er **eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten nach dem Herunterladen der Datei vornehmen muss.**

3. Keine Virenprüfung: Die zentrale Plattform kann die Virenprüfung nicht durchführen oder sie verzichtet auf Ersuchen der Benutzerin oder des Benutzers darauf.

Während der Pilotierung der zentralen Plattform hat sich gezeigt, dass die ergriffenen Schutzmassnahmen unter Umständen zu strikt sind und Dokumente aus verschiedenen Gründen zurückgewiesen wurden. Folgende Ursachen wurden während der Pilotierung identifiziert (nicht abschliessend):

- Übermittlung von passwortgeschützten oder end-2-end verschlüsselten Dateien zwischen bestimmten Behörden. Diese Dateien können prinzipiell nicht auf Schadsoftware geprüft werden, da sie verschlüsselt sind.
- Übermittlung von Dateiformaten mit Makros oder anderem ausführbaren Code: Diese enthalten zwar keine Viren im klassischen Sinne, bieten jedoch zahlreiche Angriffsmöglichkeiten für Cyberkriminelle. Aus diesem Grund werden ausführbare Dateiformate durch die Pilotplattform abgewiesen.
- Übermittlung von elektronischen Beweismitteln aus beschlagnahmten Geräten, im Original oder nach Aufbereitung durch die IT-Forensik, zum Beispiel im Rahmen der Akteneinsicht.
- Durch die ergriffenen Schutzmassnahmen werden Dateien fälschlicherweise zurückgewiesen, obwohl die Dateien von den sendenden Behörden bereinigt worden sind (sogenannte False-Positive).

In der Pilotierung wurde mehrfach gefordert, dass auch kritische Dateien übermittelt werden können, beispielsweise in einem digitalen Container. Die Behörden sollen dafür nicht auf alternative, unsichere Übermittlungswege ausweichen müssen (E-Mail, Cloud, UBS-Sticks, etc.). Die Ablage und Abholung dieser Dateien und die Prüfungen auf Schadsoftware obliegen in diesen Fällen den Nutzerinnen und Nutzern der Plattform. Wollen Sender und Empfänger auf Schutzmassnahmen verzichten, reduzieren sie die Funktion der Plattform auf die reine Übermittlung von Daten und sind selbst für den korrekten Umgang mit den Dateien verantwortlich. Dies bedingt eine ausdrückliche Absprache zwischen den Beteiligten. **Dies bedeutet auch, dass Nutzerinnen und Nutzer eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten jeweils vor und nach Übermittlung durch die zentrale Plattform vornehmen müssen.** Die Plattform muss den Empfänger zudem darauf hinweisen, dass die in einem Container übermittelten Dateien keiner Virenprüfung unterzogen worden sind.

Abs. 1

Die Festlegung der (Maximal-)Grösse von prüfbaren Blöcken grösserer Dateien sollte nicht öffentlich kommuniziert werden. Diese Information ist für die Nutzerinnen und Nutzer der Plattform irrelevant. Sie eröffnet potenziellen Angreifern die Möglichkeit, ihre Schadsoftware in einer verseuchten Datei so anzuordnen, dass der Schadcode bei der Aufspaltung in mehrere Blöcke in zwei aufeinanderfolgenden Blöcken liegt und nicht zuverlässig als schädlich erkannt werden kann. Zudem wird es stark von der für die Aufspaltung und Prüfung zuständigen Software abhängen, wie gross diese prüfbaren Blöcke zu gestalten sind. Diese Grenze wird sich aufgrund von Betriebserfahrung und Verbesserungen in der Hard- und Software dynamisch verändern und sollte einfach anpassbar sein.

Absatz 1 sollte zusammengefasst wie folgt lauten:

> [1] *Die Plattformen ~~müssen bei bis zu 64 Megabyte grossen Dateien~~ führen eine Virenprüfung durch~~führen~~.*

Abs. 2

Der Grenzwert für eine vollständige Prüfung auf Schadsoftware von derzeit 64 MB kann (und sollte) basierend auf den technischen Möglichkeiten und der wachsenden Betriebserfahrung durch die Betreiber der Plattformen erhöht werden können. **Absatz 2 ist daher zu streichen**.

> *~~[2] Dokumente ab 64 Megabyte können sie in 64 Megabyte grosse Dokumente aufteilen und diese einer Virenprüfung unterziehen.~~*

Abs. 4

Eine klare Kennzeichnung ist auch dann essenziell, wenn die Virenprüfung nur eingeschränkt stattgefunden hat. Absatz 4 ist dementsprechend zu ergänzen. Unklar ist allerdings, wie die Ergebnisse der Virenprüfung den Nutzenden mitgeteilt werden. Die Mitteilung sollte technisch einfach und inhaltlich leicht verständlich erfolgen können.

Absatz 4 sollte wie folgt lauten:

> *[4] Dokumente, bei denen ~~eine Virenprüfung nach Absatz 2~~ keine oder eine eingeschränkte Virenprüfung durchgeführt wurde, müssen entsprechend gekennzeichnet werden.*

Abs. 5

Bei der Information der Plattformen an die Absenderin oder den Absender, dass ein Dokument nicht übermittelt werden konnte, handelt es sich klarerweise nicht um eine Quittung, da eben kein Dokument übermittelt worden ist (vgl. Ausführungen zu Art. 5 Abs. 2 Bst. d Ziff. 2 oben).

6. Abschnitt: Gebühr für die Nutzung der zentralen Plattform

Basis für die Berechnung der Gebühr bilden die Artikel 6 und 32 des BEKJ. Die Kosten der zentralen Plattform werden auf die nutzenden Kantone aufgeteilt. Für die Mitglieder der Körperschaft berechnet sich der Gebührenanteil anhand der ständigen Wohnbevölkerung. Mit Nichtmitgliedern schliesst die Körperschaft eine Vereinbarung gemäss Artikel 6 BEKJ ab. Die vereinbarte Vergütung soll sämtliche Kosten decken (inklusive Investitionskosten, Botschaft BEKJ, BBl 2023 679, S. 22), welche das Nichtmitglied verursacht. Die Kosten für Nichtmitglieder werden daher in der Regel höher ausfallen als jene der Mitglieder.

Art. 15 Berechnung der Gebühr

Die deutsche und die französische Fassung wurden verglichen und vereinheitlicht; dies betrifft auch die konsistente Terminologie für denselben Sachverhalt. Für mehr Klarheit wurde der Absatz 1 in (neu) zwei Absätze aufgeteilt.

Die Dreijahresfinanzplanung als Referenz für die Festlegung des Gesamtbetrags für drei Jahre wird begrüsst. Der Ansatz liefert eine vorausschauende und realistische Grundlage für die jährlich gemäss Verteilschlüssel in Artikel 16 festzulegende Gebühr. Das ergänzende Korrektiv gemäss Absatz 4 stellt die notwendige Anpassungsfähigkeit sicher.

Folgender Text wird vorgeschlagen:

> *[1] ~~Die Gesamthöhe~~ Der Gesamtbetrag der jährlich von den Mitgliedern der öffentlich-rechtlichen Körperschaft zu entrichtenden Gebühr ~~für die Nutzung der zentralen Plattform~~ muss die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform decken und die Bildung einer Reserve für die Sicherstellung der Liquidität der öffentlich-rechtlichen Körperschaft in der Höhe von 10 Prozent der jährlichen Betriebskosten ~~ermöglichen~~ gewährleisten.*
>
> *[Anpassung und neuer Absatz 2]*
>
> *[2] ~~Die Einnahmen aus Leistungsbezügen der~~ Beiträge von Kantonen, die nicht Mitglied der öffentlich-rechtlichen Körperschaft sind, werden vom Gesamtbetrag der jährlichen Gebühr abgezogen.*

[3] Das EJPD legt ~~die jährliche~~ den Gesamtbetrag der jährlichen Gebühr ~~aufgrund~~ für jeweils drei Jahre im Voraus auf der Grundlage der Finanzplanung der öffentlich-rechtlichen Körperschaft fest.

[4] Das EJPD kann die Gebühr während der Periode nach Absatz 3 ~~2~~ anpassen, wenn die eingenommenen Beiträge nach Absatz 1 und 2 ~~diese Gebühr~~ die Betriebs- und Weiterentwicklungskosten nicht ~~deckt~~ decken oder die Reserve die Limite nach Absatz 1 überschreitet.

Art. 16 Aufteilung der Gebühr

Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 Prozent wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die Aufteilung der Gebühr sollte Gegenstand der Prüfung sein.

Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen. Anhand dieser verbindlichen Angaben legt das EJPD den jährlichen Gebührenbeitrag fest; es berücksichtig dabei die in Artikel 15 Absatz 4 definierten Schwellenwerte und den allfälligen Beitritt eines Nichtmitgliedes zur Körperschaft justitia.swiss nach deren Gründung (vgl. Art. 19 Vereinbarung justitia.swiss sowie erläuternder Bericht zur Vereinbarung justitia.swiss, S. 17).

Vorgeschlagen wird folgender Wortlaut:

[1] Die Gesamthöhe der Gebühr wird wie folgt auf den Bund und die Kantone, die Mitglied der öffentlich-rechtlichen Körperschaft sind, aufgeteilt:

a. Bundesverwaltung und Bundesanwaltschaft (BA): 5 Prozent;

b. Eidgenössische Gerichte: 5 Prozent;

c. Kantone: 90 Prozent.

[2] Der Anteil der Kantone wird ~~gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt~~ unter den Kantonen, die Mitglieder der öffentlich-rechtlichen Körperschaft sind, proportional zu deren ständigen Wohnbevölkerung am 1. Januar des Vorvorjahres, für das die Gebühr fällig wird, verteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen ~~im Zeitpunkt der Festlegung nach Artikel 15~~.

[3] Das EJPD legt jährlich die Verteilung der Gebühr auf die Kantone fest.

Art. 17 Gebührenanteil der Bundesverwaltung und der Bundesanwaltschaft

Keine Bemerkungen.

Art. 18 Gebührenanteil der eidgenössischen Gerichte

Keine Bemerkungen.

Art. 19 Fälligkeit

Die Verordnung lässt die weiteren Modalitäten der Erfüllung offen. Es ist anzunehmen, dass die Regeln des Obligationenrechts sinngemäss zur Anwendung kommen. Vorgeschlagen wird daher folgender Wortlaut der Bestimmung:

> *[1] Die jährliche Gebühr der Mitglieder der öffentlich-rechtlichen Körperschaft ist ~~sind~~ im Voraus zu entrichten und am 1. Januar fällig.*
>
> *[2] Die Gebühr für ~~das erste Betriebsjahr der öffentlich-rechtlichen Körperschaft ist an dem Tag fällig, an dem diese Verordnung in Kraft tritt~~ die Nutzung der zentralen Plattform ist erstmals am Tag des Inkrafttretens dieser Verordnung fällig.*
>
> *[3] Die Bestimmungen des Obligationenrechts zum Schuldnerverzug finden sinngemäss Anwendung.*

Art. 20 Rechnungsstelle der Kantone

Keine Bemerkungen.

Art. 21 Evaluation der Gebührenregelung

Die Überprüfung der Berechnungsweise und der Aufteilung der Gebühr wird begrüsst.

2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten

Art. 22 Digitalisierung von physischen Dokumenten

Diese Bestimmung betrifft alle Behörden, welche Verfahren leiten und deren Verfahrensrecht das BEKJ für anwendbar erklärt (Art. 2 BEKJ). Für die Kantone stehen daher die Zivilprozessordnung, das Opferhilfegesetz und die Strafprozessordnung im Vordergrund.

Das in Absatz 2 vorgeschriebene Format PDF/A erleichtert die Archivierung der Justizakten. Unklar ist, ob dieses Format durch die sehr unterschiedlichen kantonalen Justizapplikationen leicht verarbeitet werden kann.

Absatz 3 sieht die Texterkennung vor. Diese scheint in vielen Fällen sinnvoll und erleichtert die Bearbeitung der Dokumente. Bei fremdsprachigen Texten kann das Ergebnis der Texterkennung gemäss aktuellem Stand der Technik jedoch unbefriedigend oder fehlerhaft sein. Die Auflösung von 300 DPI scheint sinnvoll zu sein. Anzumerken ist, dass die Dateigrösse bei der Auflösung von 300 DPI viermal grösser ist als bei der Auflösung von 150 DPI.

Art. 22*a* (neu) Rücksendung von physischen Dokumenten

Problemstellung

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7) wird dargelegt, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Artikel 30 BEKJ in die vorliegende Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe.

Diese Feststellung bezieht sich auf die Auslegung des in Artikel 30 BEKJ enthaltenen Begriffs der «Dokumente», der im Gesetz weder weiter nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird. Eine differenzierende Betrachtung ist nach hier vertretener Auffassung aber erforderlich, um mit einer lückenhaften Verordnung zum BEKJ keine Probleme zu schaffen, die es in der analogen Welt noch gar nicht gibt. Damit ist auch gesagt, dass die anwendbaren Prozessgesetze nach hier vertretener Meinung durchaus Raum für eine Auslegung der Bestimmungen des BEKJ im Sinne ihrer gesetzgeberischen Zielsetzung lassen.

Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende

von Anzeigen in Papierform eingehen, weil derlei Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es in der analogen Welt noch gar nicht gab. Dies kann nicht der Willen des Gesetzgebers gewesen sein.

Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft, die im Schriftstück enthalten ist. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden überwiegend weggeworfen werden, sobald sie wieder bei ihren ursprünglichen Absenderinnen und Absendern eingetroffen sind.

Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, könnte mit den zurückgeschickten Dokumenten nicht Beweis geführt werden, weil sich nicht feststellen liesse, ob es auch diese Papiere waren, die gegenüber der Behörde eingereicht worden waren.

Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Artikel 30 Absatz 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Der Botschaft zum BEKJ ist zu entnehmen, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen (Botschaft BEKJ, BBl 2023 679, S. 36). Damit ist auch gesagt, dass die Rücksendepflicht von Urkunden, an deren Wiedererhalt die Absenderinnen und Absender ein Interesse haben, vorliegend nicht in Frage gestellt wird.

Hingegen braucht nicht weiter ausgeführt werden, dass durch die Auslegung des BEKJ im Sinne eines neu geschaffenen, replizierenden Postverkehrs in Papierform ein enormer Mehraufwand durch Porti und Arbeitsaufwand geschaffen wird. Eine Gesetzesauslegung, die letztlich dazu führt, dass tausende von Altpapierbündeln mit Porto versehen werden müssen, kann nicht von der gesetzgeberischen Absicht getragen sein.

Lösungsansatz

Aus den oben genannten Gründen wird vorliegend vorgeschlagen, einen neuen Artikel 22a einzufügen. Die gewählte Formulierung stellt klar, dass Dokumente, die gemäss Artikel 30 Absatz 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Artikel 30 BEKJ in die Verordnung zu schreiben. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen:

> ***2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten***
>
> […]
>
> *Art. 22a Rücksendung von physischen Dokumenten*
>
> *Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.*

Art. 22*b* (neu) Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten

Problemstellung: Wie erreicht man Personen, welche nicht auf der Plattform erreichbar sind?

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7 f.) wird ausgeführt, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Artikel 353 Absatz 1 Buchstabe k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: «Der Strafbefehl enthält: (…) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.» Artikel 238 Buchstabe h nZPO enthält eine ähnliche Regelung für zivilgerichtliche Entscheide.

Artikel 22 konkretisiert Artikel 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ zwar die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird.

Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von zehn bis zwanzig Prozent der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Zwar liegt dem BEKJ als Regulierungsgrundsatz die Idee zugrunde, dass Privatpersonen nicht zur elektronischen Kommunikation mit den Behörden gezwungen werden sollen und an dieser Grundlage soll vorliegend deshalb auch nicht gerüttelt werden. Hingegen kann es nicht richtig sein, das Unterschriftserfordernis derart restriktiv auszulegen, dass jeglichem Fortschritt ein Riegel vorgeschoben wird.

Artikel 22 Absatz 2 BEKJ ist zu entnehmen, dass künftig mittels eines geregelten elektronischen Siegels sichergestellt werden soll, dass ein elektronisch erstelltes Dokument tatsächlich von der zuständigen Behörde stammt, die sich etwa aus dem Briefkopf o.ä. ergibt. Zu diesem Artikel ist der Botschaft zum BEKJ zu entnehmen: «Das Unterschriftserfordernis stellt bei der Digitalisierung oft ein Hindernis dar. Anstelle der Unterschrift sieht das Gesetz die Authentifizierung mit Hilfe eines anerkannten elektronischen Identitätsnachweises sowie dem Anbringen eines geregelten elektronischen Siegels vor.» (Botschaft BEKJ, BBl 2023 679 S. 30). Damit ist gesagt, dass das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift ersetzt. Für einen Rückgriff auf Artikel 14 OR bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel (zum Schutzniveau vgl. Botschaft BEKJ, a.a.O.).

Lösungsansatz

Zwar ist dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens insoweit beizupflichten, dass den massgeblichen Verfahrensgesetzen zu entnehmen ist, dass etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Nach hier vertretener Auffassung lässt diese Formulierung aber durchaus eine Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes zu.

Bereits heute ist es absolut gängige Praxis bei den Zivilgerichten und den Strafbehörden, das Original der Endentscheide zu den Akten der Behörde zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen. Wie schon weiter oben zur Bestimmung über den Rückversand eingesandter Papierdokumente

ausgeführt, wird nun durch den Verzicht auf eine reduzierende Auslegung eine neue Pflicht in der analogen Welt geschaffen. Wird dem erläuternden Bericht gefolgt, soll es plötzlich eine Pflicht zum Versand von Papieroriginalen geben. Damit wird der Versand von Papieroriginalen in der digitalen Welt exponentiell vervielfacht. Das kann nicht die Idee der Gesetzgebung gewesen sein.

Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Einer Papierkopie des elektronischen Originals kommt exakt derselbe Informationsgehalt zu wie ein Entscheid, der eine handschriftliche Signatur trägt. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann.

Die vorgeschlagene Lösung hätte den Vorteil, dass in einem Verfahren keine zwei Originale desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids (ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG stellt für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Aus den in Ziffer 3.1 genannten Gründen wird deshalb vorgeschlagen, einen neuen Artikel 22b einzufügen:

> ***Art. 22b*** *Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten*
>
> *Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.*

Sollte an der viel zu engen Auslegung des BEKJ festgehalten werden, die im erläuternden Bericht skizziert ist, wäre zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen, um dem in den Verfahrensgesetzen verwendeten Begriff der «Unterschrift» genüge zu tun, obwohl diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung durch das Behördensiegel ersetzt wurde.

3. Kapitel: Elektronische Übermittlung ausserhalb einer Plattform nach dem BEKJ

1. Abschnitt: Verwendung von anderen Lösungen zur Übermittlung von Dokumenten

Art. 23 Eignungsvoraussetzungen

Diese Bestimmung konkretisiert die Artikel 128b Absatz 2 der Zivilprozessordnung, Artikel 103b Absatz 2 der Strafprozessordnung und Artikel 8c Absatz 2 des Opferhilfegesetzes vom 23. März 2007. Die Kantone gehen davon aus, dass sich diese Bestimmung an die Kommunikation zwischen Strafbehörden innerhalb der Strafprozesskette richtet, bei der Akten beispielsweise bei einem Weiterzug an die übergeordnete Instanz weitergeben müssen, wo andere Behörden mit bestimmten Verfahrenshandlungen beauftragt werden (Bsp. Ermittlungsauftrag von Staatsanwaltschaft an die Kriminalpolizei) oder bei der Übermittlung von Ergebnissen von Untersuchungshandlungen, welche die Polizei an die Staatsanwaltschaft übermittelt.

Ein zweites Anwendungsfeld ist die Zivilprozesskette, beispielsweise wenn ein Zivilgericht das Betreibungs-, das Konkursamt oder das Handelsregisteramt anweist, eine bestimmte Handlung vorzunehmen oder, wenn das erstinstanzliche Gerichte seine Akten aufgrund des Weiterzugs an die kantonale Rechtsmittelinstanz weitergibt.

Die physische Weitergabe der Akten zwischen Strafbehörden erfolgt aktuell noch oft auf dem Postweg, mit interner Post oder dem Kurierdienst. Die Beauftragung der Polizei für Untersuchungshandlung ergeht in der Regel schriftlich, jedoch werden weder genauer Zeitpunkt noch der Empfang gesondert festgehalten.

Die vorgeschlagenen Ausführungsbestimmungen orientieren sich stark an der technischen Lösung der zentralen Plattform. Bei der elektronischen Weitergabe innerhalb des Kantons (ZPO) oder unter Strafbehörden (StPO) sollten jedoch andere Anforderungen gelten als bei der Kommunikation über die zentrale Plattform.

Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank erfolgen. Dafür braucht es nach Einschätzung der Kantone keine Quittung. Die Protokollierung in den Logfiles des kantonalen IT-Systems genügen. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem mehrmaligen Versand von Dokumenten über eine externe Plattform klar vorzuziehen.

Artikel 23 sollte so ergänzt werden, damit die elektronische Weitergabe von Dokumenten durch die Mutation von Zugriffsrechten auf eine gemeinsame Datenbank zulässig ist. Die Nachvollziehbarkeit der Zeitpunkte der Übermittlung oder der Mutation von Zugriffsrechten muss gewährleistet sein. Die Anforderungen von ZPO und StPO gehen nicht so weit, dass in der digitalen Umsetzung ein synchronisierter Zeitstempel wie in Buchstabe b notwendig wäre. Deshalb ist auf dieses Kriterium zu verzichten.

Art. 24 Elektronische Übermittlung unter Behörden

Nach Einschätzung der Kantone ist die Sachüberschrift zu weit gefasst und daher irreführend. Es handelt sich stets um die Kommunikation von und zu Strafbehörden oder Zivilgerichten im Rahmen von Verfahren nach StPO oder ZPO. Gleichzeitig erscheint es erforderlich, den Begriff der übrigen Behörden, also jene, die unter das Obligatorium fallen, mit den Strafbehörden elektronisch kommunizieren zu müssen, zu definieren (vgl. Bemerkungen zu Art. 6 oben). Insbesondere mit Blick auf öffentlich-rechtliche Körperschaften, die nicht hoheitlich handeln, besteht insoweit Unklarheit.

Diese Bestimmung konkretisiert die Ausnahmen von Artikel 128c Absatz 2 der Zivilprozessordnung, Artikel 103c Absatz 2 der Strafprozessordnung und Artikel 8d Absatz 2 des Opferhilfegesetzes. Diese Ausnahmen sind dort sinnvoll, wo in Zivil- oder Strafverfahren eine grosse Anzahl von Kommunikationen mit Behörden anfallen, die nicht Teil der Straf- oder Zivilprozesskette sind und wo eine direkte Kommunikation, z.B. über eine Schnittstelle, etwa zur Weitergabe von Metadaten oder aus Kostengründen dem Rechtsverkehr über die Plattform vorzuziehen ist. Zu denken ist im Strafprozess etwa an Steuer- oder Migrationsbehörden oder auch an grosse Verkehrsbetriebe oder rechtsmedizinische Institute, die auch unter den Behördenbegriff fallen dürften. Ebenso bestimmte Behörden des Bundes wie das BAZG.

Die Voraussetzungen sollten sich an Artikel 23 orientieren und nicht darüber hinausgehen. Es ist jedenfalls nicht ersichtlich, weshalb Artikel 24 strengere Anforderungen vorsieht, da Artikel 103c Absatz 2 der Strafprozessordnung – anders als Art. 103b Absatz 2 mit der Feststellung der Zeitpunkte der Übermittlung und dem Schutz der Akte vor Veränderung und unberechtigter Kenntnisnahme - überhaupt keine Anforderungen an die Dokumentation einer Übermittlung stellt.

2. Abschnitt: Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Art. 25 Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Keine Bemerkungen.

3. Abschnitt: Elektronische Bestätigung von Protokollen im Straf- und Militärstrafprozess

Art. 26 Elektronische Bestätigung von Protokollen im Straf- und Militärstrafprozess

Keine Bemerkungen.

4. Kapitel: Schlussbestimmungen

Art. 27 Aufhebung und Änderung anderer Erlasse

Keine Bemerkungen.

Art. 28 Inkrafttreten

Die Finanzierung des Projekts Justitia 4.0, welches die zentrale Plattform im Auftrag der Kantone, des Bundes und der Justizbehörden aufbaut, ist bis Ende Jahr 2027 gesichert. Die Finanzierung von Betrieb und Weiterentwicklung der zentralen Plattform muss daher spätestens ab Anfang 2028 über Gebühren erfolgen. Die Verordnung muss gleichzeitig mit dem abschliessendem Inkrafttreten des BEKJ in Kraft gesetzt werden.

Aufhebung und Änderung anderer Erlasse

Aufhebung VeÜ-VwV

Keine Bemerkungen.

Aufhebung VeÜ-ZSSV

Durch die Aufhebung der Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren können IncaMail und PrivaSphere in Verfahren, die nach dem Inkrafttreten der Verordnung begonnen haben, nicht mehr genutzt werden. Es ist daher an den Kantonen, für Verwaltungsverfahren, welche nicht über die Plattform justitia.swiss abgewickelt werden können, geeignete Kanäle auszuwählen und bereit zu stellen.

Art. 14a VZertES Vom Validator zu prüfende Signaturen und Siegel

Keine Bemerkungen.

Art. 14b VZertES Anbringen und validieren von elektronischer Signatur und Siegel

Keine Bemerkungen.

Kanton Zürich
Regierungsrat
staatskanzlei@sk.zh.ch
Tel. +41 43 259 20 02
Neumühlequai 10
8090 Zürich
zh.ch

Elektronisch an cornelia.perler@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

10. Juni 2026 (RRB Nr. 621/2026)

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (Vernehmlassung)

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 13. März 2026 haben Sie uns eingeladen, zum Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung zu nehmen. Wir danken für diese Gelegenheit und lassen uns zu den einzelnen Bestimmungen des Vorentwurfs des VEKJ wie folgt vernehmen:

Art. 2 Anforderungen an die Plattformen

Gemäss Art. 2 Abs. 2 VEKJ regelt das Eidgenössische Justiz- und Polizeidepartement (EJPD) die funktionalen und betrieblichen Anforderungen an die Plattformen einschliesslich der Schnittstellen nach Art. 19 Abs. 1 und 2 des Bundesgesetzes über die Plattformen für die elektronische Kommunikation (BEKJ, 172.023). Der genaue Umfang dieser Delegation soll während des Vernehmlassungsverfahrens konkretisiert werden (vgl. erläuternder Bericht, S. 12). Der erläuternde Bericht hält fest, dass die Schnittstellen von der zentralen Plattform kostenlos bereitgestellt werden und sie kostenlos nutzbar sein müssen (vgl. erläuternder Bericht, S. 12). Es ist uns ein zentrales Anliegen, dass der Kanton Zürich als wichtiger Nutzer der Plattform diese Schnittstellen mitgestalten bzw. die Schnittstellenformate mitdefinieren kann. Den Kantonen sollte in Bezug auf die Schnittstellendefinition zwingend ein Mitwirkungsrecht eingeräumt werden.

Art. 3 Bewilligungsverfahren

Wir beantragen, Art. 3 Abs. 2 (der Formulierung von Abs. 4 entsprechend) wie folgt anzupassen: «[…] wenn die Anforderungen nach Artikel 25 BEKJ und Artikel 2 erfüllt sind.» Art. 3 Abs. 4 sieht vor, dass das EJPD die Bewilligung für den Betrieb von Plattformen nach Art. 1 Bst. a oder b VEKJ entzieht, wenn festgestellt wird, dass die Anforderungen nach Art. 25 BEKJ und Art. 2 VEKJ nicht mehr erfüllt sind. Aus der Bestimmung und dem

erläuternden Bericht geht nicht hervor, wie mit den auf der betreffenden Plattform gespeicherten Daten und Dokumenten im Falle eines Bewilligungsentzugs umgegangen wird (2.8. unmittelbare Löschung nach Migration auf eine andere Plattform). Dies sollte ergänzt werden.

Art. 4 Format der Dokumente

Wir beantragen, die Dateiformate in einer Departementsverordnung des EJPD zu regeln, damit rascher auf technische Neuerungen reagiert werden kann. Abs. 3 und 4 sind deshalb neu zu fassen. Dabei sollte auch der Hinweis auf die Ansetzung einer angemessenen Frist (Art. 4 Abs. 5) in Abs. 3 oder 4 integriert werden und nicht als eigener Absatz stehen bleiben.

Art. 5 Quittungen

Art. 5 Abs. 3 verlangt, dass die Angaben sowohl vom Menschen als auch von Maschinen gelesen werden können müssen. Weder das Gesetz noch die Verordnung äussern sich zur Barrierefreiheit. Wir beantragen, zu präzisieren, welche Anforderungen betreffend Barrierefreiheit gelten – sowohl für die Quittungen als auch für die Plattformen und die zu übermittelnden Dokumente.
Zudem beantragen wir, Abs. 2 Bst. d Ziff. 2 wie folgt zu ergänzen: «[…] der Virenprüfung gemäss Artikel 14 […]».

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Art. 6 VEKJ hält fest, dass es für die Übermittlung reiche, wenn nur ein Dokument über ein Siegel und einen Zeitstempel verfüge. Die Erläuterungen führen hierzu aus, dass die Behörde alle Dokumente mit einem Siegel und Zeitstempel versehen müssen. Dieser Widerspruch ist aufzulösen. Wir weisen in diesem Zusammenhang darauf hin, dass mit erheblichen Mehrkosten für die Kantone zu rechnen wäre, wenn bei der Übermittlung mehrerer Dokumente durch eine Behörde sämtliche Dokumente mit einem Siegel und einem Zeitstempel versehen werden müssten.
Gemäss Art. 22 Abs. 2 BEKJ sind Behörden verpflichtet, ihre Mitteilungen zu siegeln und mit einem Zeitstempel zu versehen. In den Erläuterungen zu Art. 6 VEKJ wird konkretisiert, dass verfahrensleitende und verfahrensbeteiligte Behörden ihre Mitteilungen siegeln und mit einem Zeitstempel versehen (vgl. erläuternder Bericht, S. 18). Verfahrensbeteiligte Behörden müssten demnach nach unserem Verständnis ebenfalls über ein Behördenprofil und nicht bloss – wie nach unserem bisherigen Informationsstand – über ein Organisationsprofil verfügen. Dies ist für die Umsetzung in den Kantonen von erheblicher Bedeutung und wir würden eine entsprechende Klarstellung begrüssen. Für Behörden, die typischerweise nicht als verfahrensleitende Behörden auftreten, ist ein Behördenprofil grundsätzlich weder erforderlich noch sachgerecht. Aus unserer Sicht wäre deshalb zielführend, wenn die Siegelungspflicht nur die verfahrensleitende und nicht auch die verfahrensbeteiligte Behörde treffen würde. Würde an der Siegelpflicht für alle Behörden gemäss erläuterndem Bericht festgehalten, so müssten alle Schweizer Behörden auf allen Stufen mit einem Siegel ausgestattet werden. Für die flächendeckende Ausstattung aller Schweizer Behörden mit einem elektronischen Siegel liefert das BEKJ keine genügende gesetzliche

Grundlage. Für die Kantone wäre zudem eine flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden.

Art. 7 Siegelung der Dokumente durch die Plattform

Wir beantragen, Art. 7 zum besseren Verständnis wie folgt anzupassen: «Werden mehrere Dokumente übriger Benutzerinnen und Benutzer zusammen übermittelt, […]».

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Art. 12 sieht vor, dass Dokumente und Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch vernichtet werden.
Die automatisierte Löschung von Dokumenten nach einer überschaubaren Zeitspanne ist grundsätzlich zu begrüssen, allerdings ist die maximale Aufbewahrungsfrist von sechs Monaten für auf der Plattform gespeicherte Dokumente und Quittungen zu kurz. Es ist weder zielführend noch effizient, wenn Dokumente strikt nach spätestens sechs Monaten gelöscht werden. Strittige Verfahren dauern in der Regel länger als sechs Monate, was in der Praxis dazu führen würde, dass eine verfahrensleitende Behörde sechs Monate nach Beginn eines Verfahrens immer wieder prüfen müsste, ob ihre Akte auf der Plattform noch aktuell ist oder ob sie bestimmte Dokumente allenfalls wieder hochladen muss. Das Problem zeigt sich insbesondere in Bezug auf die Quittungen: Quittungen können sehr spät im Verfahren benötigt werden, etwa um die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen. Unterbleibt das Herunterladen einer Quittung von der Plattform innert der Frist von sechs Monaten, wird sie irreversibel gelöscht und, da sie direkt aus dem System geschaffen wird, ist es auch nicht möglich, sie aus einer anderen Quelle wieder herzustellen. Wir beantragen deshalb, die Löschfrist von sechs Monaten zu verlängern.

Art. 16 Aufteilung der Gebühr

Gemäss dem erläuternden Bericht (S. 28) ist für den Betrieb und die Weiterentwicklung der zentralen Plattform mit jährlichen Kosten von 10 Mio. bis 12 Mio. Franken zu rechnen. Aufgrund der vorgesehenen Gebühren- bzw. Kostenaufteilung (10% Bund, 90% Kantone; vgl. Art. 16 Abs. 1 VEKJ) entfielen davon 9 Mio. bis 10,8 Mio. Franken auf die Kantone. Unter den Kantonen sollen diese Kosten im Verhältnis der ständigen Wohnbevölkerung aufgeteilt werden (vgl. Art. 16 Abs. 2 VEKJ). Ende 2025 betrug der Anteil des Kantons Zürich an der ständigen Wohnbevölkerung der Schweiz rund 18%. Der Kanton Zürich hätte deshalb mit jährlichen Kosten in der Grössenordnung von rund 1,6 Mio. bis 1,9 Mio. Franken zu rechnen.
Die rechtlichen Vorgaben zur Nutzung der Plattform werden vom Bund erlassen. Die vorgesehene Kostenbeteiligung des Bundes von lediglich 10% widerspricht deshalb dem Prinzip der fiskalischen Äquivalenz (Art. 43a Abs. 3 Bundesverfassung [SR 101]). Wir fordern deshalb eine Kostenbeteiligung des Bundes von mindestens 50%. Zudem weisen wir darauf hin, dass die Notwendigkeit, justizielle Verfahren zu digitalisieren, in allen Kantonen gleichermassen besteht. Es ist deshalb nicht angezeigt, die Aufteilung der Kosten für den Aufbau ausschliesslich im Verhältnis zur Bevölkerungszahl zu berechnen. Vielmehr ist auch ein Sockelbeitrag vorzusehen.

Art. 23 Eignungsvoraussetzung

Art. 103b Abs. 1 StPO sieht im Grundsatz vor, dass die Strafbehörden (Art. 12 StPO) die Akten über eine Plattform nach dem BEKJ weitergeben sollen. Unter Einhaltung der Voraussetzungen von Art. 103b Abs. 2 Bst. a und b StPO, die nun in Art. 23 VEKJ konkretisiert sind, können auch andere Lösungen eingesetzt werden.
Demnach ist die Übermittlung unter Strafbehörden auch erlaubt, wenn der Zeitpunkt der Übermittlung festgehalten wird (Bst. a), ein synchronisierter Zeitstempel verwendet wird (Bst. b) und die Akten bei der Übermittlung und in der Ablage vor Veränderung und unberechtigter Kenntnisnahme geschützt sind (Bst. c). Sind diese Voraussetzungen nach Art. 23 erfüllt, ist die Verwendung von «anderen Lösungen» zur Übermittlung von Dokumenten unter Strafbehörden möglich (erläuternder Bericht, S. 32). Weitere Zustellplattformen als die in Art. 3 BEKJ vorgesehenen unterliegen jedoch dem Vorbehalt der Bewilligung durch das EJPD. Aus der Vorlage und dem erläuternden Bericht ergibt sich dabei nicht, ob auch Plattformen, die nur innerkantonal zwischen Strafbehörden für die Übermittlung von Daten genutzt werden, unter diese Bewilligungspflicht durch das EJPD fallen. Hier wäre eine Präzisierung wünschenswert, beispielsweise in der im erläuternden Bericht angekündigten Departementsverordnung des EJPD.

Ergänzend ist auf folgende Punkte hinzuweisen:

Rücksendung von Dokumenten

Gemäss Art. 30 Abs. 1 BEKJ senden die Behörden die physisch eingereichten Dokumente nach der Digitalisierung an die Absenderin oder den Absender zurück. Im Strafprozess werden solche Dokumente heute nur in Ausnahmefällen an die Absenderin oder den Absender retourniert. Dies soll auch künftig möglichst beibehalten werden. Wir beantragen deshalb eine Ergänzung der VEKJ mit einer entsprechenden Bestimmung.

Zustellung von Papierkopien

In den Strafverfahren wird von Verfügungen und Beschlüssen in der Regel ein Original ausgefertigt, das zu den Akten genommen wird. Die Parteien erhalten nicht handschriftlich unterzeichnete Papierkopien. Dies sollte auch in Zukunft so möglich sein. Wir beantragen deshalb die Ergänzung der VEKJ mit einer entsprechende Bestimmung.

Anpassung der Zivilstandsverordnung vom 28. April 2004

Mit dem BEKJ wurde eine Pflicht zur elektronischen Kommunikation für die professionellen Rechtsanwenderinnen und -anwender eingeführt, wozu auch die Anwaltschaft gehört. Eine Pflicht zur elektronischen Verfahrensführung für Anwältinnen und Anwälte kennt auch das revidierte Verwaltungsrechtspflegegesetz des Kantons Zürich, das am 1. Januar 2027 in Kraft tritt. Art. 89 Abs. 5 der Zivilstandsverordnung (ZStV; SR 211.112.2) sieht hingegen vor, dass eine elektronische Verfahrensführung nur mit Einverständnis der Parteien möglich ist. Art. 89 Abs. 5 ZStV geht dabei den kantonalen Verfahrensnormen vor. Zudem schreibt Art. 89 Abs. 4 ZStV – ebenfalls entgegen den Vorgaben des BEKJ bzw. der VEKJ – zwingend die Nutzung einer qualifizierten elektronischen Signatur vor. Um Rechtsunsicherheiten zu vermeiden, beantragen wir deshalb, im Sinne einer Nebenänderung Art. 89 ZStV anzupassen und mit den Vorgaben des BEKJ bzw. der VEKJ in Einklang zu bringen.

Anpassung der Handelsregisterverordnung vom 17. Oktober 2007

Mit Anhang I hebt der Vorentwurf die Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV) auf. Unter anderem verweist aber Art. 12b der Handelsregisterverordnung (SR 221.411) weiterhin auf diese aufzuhebende Verordnung. Wir regen dazu an, dies als Anlass zu nehmen, um die Formvorschriften für das Handelsregister generell praxistauglicher und kundenfreundlicher neu zu konzipieren.

Inkrafttreten

Gemäss Art. 37 Abs. 1 BEKJ können Nutzende ab dem Inkrafttreten der abschliessenden Inkraftsetzung freiwillig elektronische Eingaben über die Plattform einreichen. Dies setzt voraus, dass die betroffenen Behörden zu diesem Zeitpunkt über die Plattform erreichbar sind und die Anforderungen des BEKJ sowie der VEKJ zumindest für den Empfang elektronischer Eingaben umgesetzt haben. Vor diesem Hintergrund erscheint ein Inkrafttreten per Mitte 2027 als sachgerecht.

Freundliche Grüsse

Im Namen des Regierungsrates

Die Präsidentin: Der stv. Staatsschreiber:

Carmen Walker Späh Dr. Peter Hösli

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Sécrétariat général
Postfach, 3001 Bern / www.svp.ch
Tel. 031 300 58 58 / gs@svp.ch
IBAN: CH80 0900 0000 3000 8828 55

Département fédéral de justice et police DFJP
Monsieur le Conseiller fédéral
Beat Jans

Par courrier électronique :
cornelia.perler@bj.admin.ch

Berne, le 22 juin 2026

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Réponse de l'UDC Suisse à la procédure de consultation

Monsieur le Conseiller fédéral,

Mesdames et Messieurs,

L'UDC Suisse vous remercie de l'avoir consultée au sujet de l'objet cité en titre. Après avoir examiné les détails du projet, elle a l'avantage de se prononcer comme suit :

L'UDC rejette clairement le présent projet. Elle considère que ce dernier n'est pas à la hauteur des enjeux qu'il entend régler et qu'il révèle des lacunes techniques et réglementaires, notamment en matière de sécurité informatique et de validation des signatures électroniques. Dans un domaine aussi sensible, de telles insuffisances ne peuvent être tolérées. L'UDC déplore en outre que le projet sous-estime systématiquement les charges financières liées à sa mise en œuvre.

L'ordonnance vise à mettre en œuvre la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ) en précisant les règles nécessaires à son application concrète. Le projet d'ordonnance porte en particulier sur les conditions d'autorisation pour exploiter une plateforme, sur les moyens d'authentification des utilisateurs, sur les formats et tailles de documents admis ainsi que sur le montant et la perception d'un émolument pour la plateforme centralisée.

S'agissant de la sécurité des données, le rapport explicatif reconnaît lui-même que l'évolution de la société en société de l'information comporte des risques dont la complexité et le dynamisme sont croissants. Si l'UDC partage ce constat, nous ne pouvons que nous montrer critiques envers certaines lacunes techniques que comporte le projet. En effet, alors que la diversification des facteurs d'identification permettrait de limiter les risques, AGOV est présenté comme étant le moyen central d'authentification, ce qui crée une dépendance technique sensible, pouvant accroître les conséquences potentielles d'un incident de sécurité. Cette dépendance est d'autant plus préoccupante que le rapport admet lui-même que des renoncements aux contrôles antivirus pourront être accordés par les exploitants de la plateforme. L'UDC est consciente des complexités techniques évoquées, mais au vu de la grande sensibilité des données traitées et de l'importance systémique de la plateforme, il n'est pas acceptable de tolérer le moindre risque sécuritaire, fût-ce en permettant de tels renoncements, même dans les cas présentés comme justifiés.

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Sécrétariat général
Postfach, 3001 Bern / www.svp.ch
Tel. 031 300 58 58 / gs@svp.ch
IBAN: CH80 0900 0000 3000 8828 55

Au-delà de la sécurité technique de la plateforme, la sécurité juridique des actes transmis constitue également un élément central. L'UDC déplore à ce titre que la validation des signatures électroniques, pierre angulaire de l'authenticité des actes judiciaires numériques, ne fasse pas l'objet d'un encadrement plus contraignant. Le rapport reconnaît en effet que l'un des principaux problèmes rencontrés en la matière réside dans la marge de manœuvre importante laissée par les normes techniques internationales, qu'il qualifie lui-même de « source de problèmes ». Malgré cela, l'art. 14b renvoie à ces mêmes normes techniques internationales et présente un caractère potestatif. Pour l'UDC, il est par conséquent inacceptable qu'un problème ainsi identifié ne donne lieu qu'à une disposition aussi peu précise dans l'ordonnance. Afin de garantir des validations souveraines, uniformes et juridiquement sûres, il conviendrait d'assortir l'art. 14b de garanties plus claires.

Sur le plan des coûts, l'UDC constate que le présent projet d'ordonnance sous-estime systématiquement les charges financières qu'il génère. S'agissant des avocats, le rapport reconnaît que ceux-ci sont concernés au premier chef par l'obligation de communiquer par voie électronique, puisqu'ils ne pourront plus déposer leurs actes de procédure et pièces jointes sur papier auprès des tribunaux et des autorités, mais devront le faire exclusivement par voie électronique. Malgré ce constat, le rapport se limite à indiquer que cette nouveauté « n'entraîne pas impérativement des coûts supplémentaires » ; tout en admettant que de tels coûts peuvent découler de l'adaptation de l'infrastructure, d'un besoin de personnel supplémentaire ou d'une augmentation du temps nécessaire pour effectuer certaines tâches. Pour une étude d'avocats de petite taille, les facteurs cités ne sont pas hypothétiques, ils sont quasi inévitables. L'usage du conditionnel ne saurait donc masquer la réalité de la charge financière qui s'imposera aux praticiens. Cette même tendance à minimiser les coûts se retrouve dans le système d'émoluments prévu, auquel l'UDC s'oppose, dans la lignée de sa prise de position de 2021 sur la LPCJ. Il n'est pas admissible de faire peser sur les cantons l'essentiel des coûts d'un dispositif centralisé dont l'efficacité demeure incertaine, alors même que ces émoluments pourraient encore augmenter en cas de hausse inattendue des frais.

Pour ces raisons, l'UDC rejette clairement ce projet qui ne présente pas les garanties minimales requises en matière de sécurité technique, de sécurité juridique et de maîtrise des coûts.

Réitérant ses remerciements de l'avoir associée à cette consultation, l'UDC Suisse vous prie de croire, Monsieur le Conseiller fédéral, Mesdames et Messieurs, à l'assurance de sa considération.

Avec nos meilleures salutations

UNION DÉMOCRATIQUE DU CENTRE

Le président du parti

Marcel Dettling

Conseiller national

Le secrétaire général

Henrique Schneider

AARGAUISCHER ANWALTSVERBAND

A-Post plus (A+)
Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz BJ
Bundesrain 20
CH-3003 Bern

Aarau, 22. Juni 2026

Vernehmlassung zum Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrte Damen und Herren

Der Aargauer Anwaltsverband dankt für die Gelegenheit, zum Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VE-VEKJ) Stellung zu nehmen.

Unser Verband unterstützt die Zielsetzung, den elektronischen Rechtsverkehr schweizweit einheitlich, sicher und praxistauglich auszugestalten. Gerade weil die Digitalisierung der Justiz für die Anwaltschaft künftig obligatorisch sein wird, ist jedoch sicherzustellen, dass die neuen Regelungen die Berufsausübung nicht unverhältnismässig erschweren, keine Rechtsunsicherheiten schaffen und den Zugang zum Recht nicht beeinträchtigen. Der erläuternde Bericht hält selbst fest, dass die Anwaltschaft vom Obligatorium besonders stark betroffen ist und Rechtsschriften sowie Beilagen künftig nur noch elektronisch einreichen können wird.

Aus Sicht des Aargauer Anwaltsverbandes besteht insbesondere in folgenden Punkten Anpassungsbedarf.

1. Allgemeine Bemerkung: Mehraufwand auf Seiten der Anwaltschaft

Mit dem Projekt Justitia 4.0 werden zahlreiche Arbeitsschritte, die bislang ganz oder teilweise bei Behörden und Gerichten anfielen, aufgrund der Pflicht zur elektroni-

Cordulaplatz 3
5400 Baden
Telefon +41 (0)62 823 40 50
Telefax +41 (0)62 823 40 51
info@anwaltsverband-ag.ch

schen Übermittlung von berufsmässig handelnden Personen faktisch auf die Anwaltschaft verlagert. Dazu gehören namentlich das Scannen und Aufbereiten von Papierunterlagen, die Strukturierung elektronischer Beilagen, die Bewirtschaftung von Übermittlungsplattformen, die Kontrolle von Metadaten, der Umgang mit Dateiformaten und Dateigrössen sowie zusätzliche Anforderungen an IT-Sicherheit und Kanzleiorganisation.

Der erläuternde Bericht zur VE-VEKJ hält fest, die Änderung der Arbeitsweise führe «nicht zwangsläufig» zu Mehrkosten; mögliche Mehrkosten könnten durch Infrastruktur, Personalbedarf oder erhöhten Zeitaufwand entstehen. Diese Einschätzung greift unseres Erachtens zu kurz. Jedenfalls für kleinere und mittlere Kanzleien ist absehbar, dass die obligatorische elektronische Kommunikation erhebliche organisatorische, technische und personelle Zusatzaufwände verursachen wird.

2. Art. 2 Abs. 1 lit. c VE-VEKJ: Dateigrösse und technische Begrenzungen

Art. 2 Abs. 1 lit. c VE-VEKJ sieht vor, dass die Plattform bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln kann. Diese Mindestanforderung ist zu begrüssen. Sie genügt jedoch nicht, wenn daneben weitere technische Begrenzungen durch Plattformbetreiber zugelassen werden oder grössere Dateien nur nach freiem Ermessen übermittelt werden können.

Antrag:
Art. 2 Abs. 1 lit. c VE-VEKJ sei wie folgt zu ergänzen:

Die Plattform kann bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln. Weitere technische Begrenzungen sind nicht zulässig. Die Betreiberinnen der Plattformen erteilen Rechtsanwältinnen und Rechtsanwälten auf Anfrage die Berechtigung, grössere Dateien zu übermitteln, soweit dies für die Wahrung der Interessen der vertretenen Partei erforderlich ist.

Begründung:
Gerade in umfangreichen Zivil-, Straf- und Verwaltungsverfahren können elektronische Beweismittel, Bild-, Audio-, Video- oder Archivdateien die Schwelle von zwei Gigabyte überschreiten. Der erläuternde Bericht verweist zwar darauf, dass grössere Dokumente aufgeteilt werden könnten. Eine solche Aufteilung ist in der Praxis aber nicht immer zweckmässig und kann insbesondere bei strukturierten Daten, forensischen Datenträgerabbildern oder umfangreichen elektronischen Beweismitteln zu Problemen bei Integrität, Nachvollziehbarkeit und Beweiswürdigung führen.

Es muss deshalb in der Verordnung selbst klargestellt werden, dass die Zwei-Gigabyte-Grenze keine starre Obergrenze darstellt und dass Rechtsanwältinnen und Rechtsanwälte bei Bedarf Anspruch auf eine technische Lösung zur Übermittlung grösserer Dateien haben.

3. Art. 4 Abs. 2 VE-VEKJ: Beilagen in jedem Format

Art. 4 Abs. 2 VE-VEKJ hält fest, dass Beilagen in jedem Format übermittelt werden können. Diese Regelung wird ausdrücklich begrüsst. Sie ist zentral für eine echte Digitalisierung des Rechtsverkehrs. Elektronische Beweismittel entstehen in der Praxis in sehr unterschiedlichen Formaten. Eine Pflicht zur vorgängigen Konvertierung würde nicht nur Aufwand verursachen, sondern kann auch Beweiswert und Integrität beeinträchtigen.

Art. 4 Abs. 2 VE-VEKJ ist daher beizubehalten.

4. Art. 4 Abs. 3 VE-VEKJ: Liste zwingend bearbeitbarer Formate

Art. 4 Abs. 3 VE-VEKJ enthält eine Liste von Dateiformaten, welche die verfahrensleitende Behörde bearbeiten können muss.

Antrag:
Art. 4 Abs. 3 VE-VEKJ sei ersatzlos zu streichen.

Begründung:
Die vorgesehene Liste ist zu eng und sachlich nicht überzeugend. Sie enthält zwar gängige Formate, lässt aber ebenfalls verbreitete und praxisrelevante Dateitypen ausser Acht, etwa TIFF, TXT, HTML, SVG oder weitere strukturierte Datenformate. Gerade HTML-Dateien können in Straf- und Zivilverfahren eine erhebliche Rolle spielen, beispielsweise bei Exporten aus sozialen Medien, Webseiten oder Kommunikationsplattformen.

Die Gefahr besteht, dass die Liste in der Praxis nicht als Mindeststandard, sondern als abschliessender Katalog verstanden wird. Damit würde Art. 4 Abs. 2 VE-VEKJ, wonach Beilagen in jedem Format übermittelt werden können, faktisch relativiert. Dies schafft Rechtsunsicherheit und öffnet einem uneinheitlichen Umgang mit elektronischen Beweismitteln Tür und Tor.

5. Art. 4 Abs. 4 und 5 VE-VEKJ: Nachforderung anderer Formate

Art. 4 Abs. 4 VE-VEKJ sieht vor, dass die verfahrensleitende Behörde die einreichende Person auffordern kann, eine Beilage in einem von der Behörde festgelegten Format einzureichen oder den Zugriff in geeigneter Weise zu ermöglichen, wenn sie die Beilage nicht zweckmässig bearbeiten kann. Der erläuternde Bericht hält zudem fest, einzelne Gerichte und Behörden könnten in Merkblättern festhalten, welche Formate von ihnen verwendet werden können.

Antrag:
Art. 4 Abs. 4 und 5 VE-VEKJ seien ersatzlos zu streichen.

Begründung:
Die vorgeschlagene Regelung führt zu einem Flickenteppich. Wenn jede Behörde und jedes Gericht eigene technische Merkblätter erlässt, entsteht keine Harmonisierung, sondern eine Deharmonisierung des elektronischen Rechtsverkehrs. Anwältinnen und Anwälte müssten vor jeder Einreichung prüfen, welche Formate die konkret zuständige Behörde akzeptiert oder bearbeiten kann. Dies widerspricht dem Ziel eines schweizweit einheitlichen elektronischen Rechtsverkehrs.

Hinzu kommt, dass Anwältinnen und Anwälte das Format elektronischer Beweismittel häufig nicht frei bestimmen. Elektronische Beweismittel sind grundsätzlich in der Form einzureichen, in der sie vorliegen. Eine Konvertierung kann Metadaten verändern, Inhalte verfälschen oder den Beweiswert beeinträchtigen. Gerade aus Gründen der Nachvollziehbarkeit und der Beweismittelintegrität ist es problematisch, wenn die einreichende Partei gezwungen wird, elektronische Beweismittel in ein anderes Format zu überführen.

Behörden und Gerichte müssen im Zuge der Digitalisierung in die Lage versetzt werden, elektronische Beweismittel sachgerecht entgegenzunehmen, zu prüfen und zu würdigen. Die technische Unzulänglichkeit einzelner Behörden darf nicht dazu führen, dass Parteien oder ihre Rechtsvertretungen das Risiko und den Aufwand der Formatkompatibilität tragen.

6. Art. 5 Abs. 2 lit. d Ziff. 2 VE-VEKJ / Art. 14 Abs. 5 VE-VEKJ

Gemäss Art. 14 Abs. 5 VE-VEKJ darf ein Dokument, bei dem aufgrund der Virenprüfung ein Virus vermutet wird, nicht übermittelt werden. Die Plattform informiert die Absenderin oder den Absender darüber, dass das Dokument nicht übermittelt wurde. Die Eingangsquittung gemäss Art. 5 Abs. 2 lit. d Ziff. 2 VE-VEKJ enthält in diesem Fall

lediglich eine «Liste der aufgrund des Resultats der Virenprüfung nicht übermittelten Dokumente und deren Grösse».

Antrag:

Art. 14 Abs. 5 VE-VEKJ sei dahingehend anzupassen, dass auch aufgrund eines Virenverdachts nicht an die Plattform übermittelte Dokumente als eingereicht gelten. Art. 5 Abs. 2 lit. d Ziff. 2 VE-VEKJ sei dahingehend anzupassen, dass auch für die nicht übermittelten Dokumente die Hashwerte auf der Eingangsquittung ausgewiesen werden. Zudem sei die Pflicht der Behörde, in Fällen aufgrund des Resultats der Virenprüfung nicht übermittelter Dokumente eine gerichtliche Nachfrist zur Verbesserung anzusetzen, in der Verordnung ausdrücklich festzuhalten.

Begründung:

Gemäss der vorgesehenen Regelung gelten Dokumente, bei denen aufgrund der Virenprüfung ein Virus vermutet wird, faktisch als nicht eingereicht. Die Angaben auf der Eingangsquittung (Dateiname und Grösse) erlauben dabei keine eindeutige Identifikation des betroffenen Dokuments. Die Verordnung regelt sodann nicht ausdrücklich, wie in einem solchen Fall weiter vorzugehen ist, sondern verweist lediglich auf die bestehenden prozessualen Bestimmungen betreffend mangelhafte Eingaben (z.B. Art. 132 Abs. 1 ZPO).

Diese Regelung ist aus Sicht der Anwaltschaft unbefriedigend und schafft Rechtsunsicherheit. Gleichzeitig fehlt mangels Ausweisung des Hashwerts die Möglichkeit, eindeutig nachzuweisen, welches Dokument eingereicht werden sollte. Zur Gewährleistung der Rechtssicherheit sollte daher klargestellt werden, dass auch von der Virenprüfung zurückgewiesene Dokumente als eingereicht gelten, deren Hashwerte auf der Eingangsquittung ausgewiesen werden und die Behörde eine Nachfrist zur Behebung des Mangels anzusetzen hat.

7. Fehlende Regelung zu Schnittstellen

Art. 10 VE-VEKJ regelt lediglich, dass der technische Zugang über eine Schnittstelle als Berechtigung nach Art. 24 Abs. 1 BEKJ gilt. Der VE-VEKJ enthält hingegen keine materiellen Anforderungen an Schnittstellen. Dies ist ungenügend. Art. 19 Abs. 3 BEKJ sieht ausdrücklich vor, dass der Bundesrat die Anforderungen an die Schnittstellen regelt.

Antrag:
Der VE-VEKJ sei um eine Bestimmung zu den Anforderungen an Schnittstellen zu ergänzen. Dabei seien insbesondere die Bedürfnisse der Anwaltschaft und der Anbieter anwaltlicher Fachapplikationen zu berücksichtigen.

Begründung:
Die Anwaltschaft wird voraussichtlich eine der grössten Nutzergruppen der Plattform justitia.swiss sein. Für eine praxistaugliche Nutzung ist entscheidend, dass Kanzleisoftware und andere Fachapplikationen über stabile, dokumentierte, sichere und diskriminierungsfrei zugängliche Schnittstellen angebunden werden können.

Die Schnittstellen müssen so ausgestaltet sein, dass Eingaben, Beilagen, Quittungen, Zustellungen, Fristenkontrolle und Aktenbewirtschaftung effizient in bestehende Kanzleiprozesse integriert werden können.

8. Schlussbemerkung

Der Aargauer Anwaltsverband unterstützt die Digitalisierung der Justiz. Sie kann jedoch nur gelingen, wenn sie praxistauglich, rechtsstaatlich abgesichert und für die betroffenen Berufsgruppen tragbar umgesetzt wird.

Wir ersuchen Sie daher höflich, die vorstehenden Anträge im weiteren Verfahren zu berücksichtigen.

Freundliche Grüsse

Aargauer Anwaltsverband



Dr. iur. Matthias Brunner

Präsident

Kopie zu den Verbandsakten.

ADVOKATENKAMMER BASEL

Bundesamt für Justiz
Cornelia Perler

übermittelt per Mail an
cornelia.perler@bj.admin.ch

Basel, 20. Juni 2026

AG | andrea.gysin@akbs.ch / andrea.gysin@gysinrecht.ch

Vernehmlassungsantwort zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Frau Perler
Sehr geehrte Damen und Herren

Wir beziehen uns auf die oben erwähnte, am 13. März 2026 eröffnete Vernehmlassung. Die Advokatenkammer Basel vertritt die Interessen ihrer Mitglieder, die von der rubrizierten Vorlage durch das im BEKJ verankerte Obligatorium stark betroffen sind.

Die Advokatenkammer Basel unterstützt die Stellungnahme des Bernischen Anwaltsverbandes vollumfänglich. Herausstreichen möchten wir insbesondere den nachfolgenden Punkt:

- **Fehlende Regelung der Kostenfrage auf Anwaltsseite**

Mit dem Projekt Justitia 4.0 werden zahlreiche Tätigkeiten von den Behörden an die Anwaltschaft ausgelagert (Scannen, Erfassen von Metadaten, Dateianalysen, Bewirtschaftung von Plattformen, Anwaltskanzleien als Unterlagendrehscheiben etc.). Das Scannen von Papierunterlagen beispielsweise ist ein aufwändiger und fehleranfälliger Prozess. Das Scannen nach TR Resiscan führt zu Kosten von bis zu 90 Rappen/Seite. **Es muss sichergestellt werden, dass alle neu auf die Anwaltschaft abgewälzte Aufwände kostendeckend abgegolten werden**. Diese Frage darf nicht den kantonalen Gerichten oder Regierungen überlassen werden, sondern muss als zentraler Teil des Vorhabens Justitia 4.0 gesamtschweizerisch geregelt werden.

Wir bitten höflich um Berücksichtigung unserer Anliegen und Anträge gemäss der Eingabe des Bernischen Anwaltsverbands.

Besten Dank und

freundliche Grüsse
ADVOKATENKAMMER BASEL



lic. iur. Andrea Gysin, Advokatin
Präses

bavaab
Bernischer Anwaltsverband
Association des avocats bernois

Per Email an cornelia.perler@bj.admin.ch
Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Beat Jans, Bundesrat

Burgdorf, 22. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) / Vernehmlassung

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Im Namen des Bernischen Anwaltsverbands (BAV) lassen wir Ihnen im Vernehmlassungsverfahren zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) gerne vorliegende Stellungnahme zukommen.

Der Vorstand des Bernischen Anwaltsverbandes dankt Herrn RA Daniel Kettiger, Herrn RA Tobias Weber, Herrn RA Nicolas Bischoff sowie Frau RA Claudia Schreiber für die Erarbeitung der vorliegenden Stellungnahme sowie allen weiteren Personen, die dem BAV Rückmeldungen zum VE VEKJ übermittelt haben, für das Engagement zugunsten einer echten Digitalisierung der Justiz. Der Vorstand des Bernischen Anwaltsverbandes ersucht Sie, sehr geehrter Herr Bundesrat, sehr geehrte Damen und Herren, höflich, die Anliegen zu berücksichtigen und dankt Ihnen für die Möglichkeit zur Stellungnahme bestens.

Mit freundlichen Grüssen

Bernischer Anwaltsverband

Véronique Bachmann, Fürsprecherin
Geschäftsführerin BAV

BAV AAB
Bernischer Anwaltsverband
Association des avocats bernois

Sekretariat
Platanenstrasse 2
Postfach 1052
3401 Burgdorf

Telefon 034 423 11 89
Fax 034 423 11 92
info@bav-aab.ch
www.bav-abb.ch

bavaab
Bernischer Anwaltsverband
Association des avocats bernois

Vernehmlassung 2024/79

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Stellungnahme des Bernischen Anwaltsverbands BAV zum Vorentwurf VE-VEKJ

Inhaltsverzeichnis

1 Die Aktivitäten des BAV i.S. Digitalisierung der Justiz 3

2 Leitsätze 3

2.1 Einleitung, Verweis auf Anhang zu diesem Dokument 3

3 Generelle Bemerkungen 3

3.1 Erläuterungen zum VE-VEKJ 3

3.2 Begrifflichkeit 3

3.3 Ungerechtfertigte dominante Rolle von EJPD/BJ 4

3.4 Gemeinsame Verordnung für Plattform nach Art. 6a VwVG und für Plattformen nach BEKJ wird abgelehnt 4

3.5 Handhabung von Rechtsetzungsdelegationen 4

3.6 Kostenfrage auf Anwaltsseite ausgeblendet 6

3.7 Business Continuity, alternative Formen der Übermittlung im Notfall 6

4 Kommentare zu Titel, Ingress und zu den einzelnen Artikeln 6

4.1 Titel der Verordnung 6

4.2 Ingress 7

4.3 Zum Kapitel 1 «Ausgangslage» des erläuternden Berichts 7

4.4 Zum Kapitel 2.3 des erläuternden Berichts 7

4.5 Zum Kapitel 2 des erläuternden Berichts 7

4.6 Artikel 1 7

4.7 Artikel 2 9

4.8 Artikel 3 11

4.9 Artikel 4 12

4.10 Artikel 5 16

4.11 Artikel 6 17

4.12 Artikel 7 18

4.13 Artikel 8 18

4.14 Artikel 9 19

4.15 Artikel 10 20

4.16 Artikel 11 20

4.17 Artikel 12 21

4.18 Artikel 13 22

4.19 Artikel 14 22

4.20 Artikel 15 bis 21 23

4.21 Artikel 22 23

4.22 Artikel 23 27

4.23 Artikel 24 29

4.24 Artikel 25 30

4.25 Artikel 26 30
4.26 Kapitel X (neu). Eindeutige Identifikation von Aktenstücken 30
4.27 Stellungnahme zum Anhang 1 VE-VEKJ....31
5 Anhang 32
5.1 Leitsätze....32

1 Die Aktivitäten des BAV i.S. Digitalisierung der Justiz

Der Bernische Anwaltsverband (BAV) steht der Digitalisierung der Justiz offen gegenüber und bringt sich aktiv in Diskussionen ein. Er arbeitet seit einiger Zeit aktiv auf eine Digitalisierung von Anwaltschaft und Justiz hin. Der BAV bietet seinen Mitgliedern seit Jahren Weiterbildungen in diesem Bereich an (bspw. Crashkurs Justitia 4.0 und Einführung in die elektronische Anwaltskanzlei, BAV Digitalmittag online-Veranstaltungen, etc.). Der BAV unterhält auch eine Sprechstunde Digitalisierung, die den Mitgliedern unentgeltlich zur Verfügung steht.

Als Berufsverband ist es aber Aufgabe des BAV, die Interessen seiner Mitglieder zu wahren und deshalb Digitalisierungsschritte im Justiz- und Verwaltungsbereich aus Anwendersicht, aus der Perspektive des Berufsstandes sowie aus Sicht nicht anwaltlich vertretener Bürgerinnen und Bürger kritisch zu beleuchten.

2 Leitsätze

2.1 Einleitung, Verweis auf Anhang zu diesem Dokument

Im Vorfeld der Vernehmlassung zum Vorentwurf des BEKJ wurden 2020/2021 durch eine Gruppe von Rechtsanwält:innen Leitsätze zum Projekt Justitia 4.0 definiert. Diese Leitsätze werden im Anhang vorgestellt.

3 Generelle Bemerkungen

3.1 Erläuterungen zum VE-VEKJ

Gemäss Art. 26 PublV werden Erläuterungen zu Verordnungen und Verordnungsänderungen in der Amtlichen Sammlung des Bundesrechts (AS) veröffentlich, Dies jedenfalls dann, wenn ein Vernehmlassungsverfahren stattgefunden hat. Die Erläuterungen zum VEKJ werden somit künftig als Materialien bei der Auslegung und Anwendung der VEKJ eine massgebliche Rolle spielen. Mit den Erläuterungen kann die Bundesverwaltung auf die künftige Anwendung der VEKJ Einfluss nehmen. Deshalb werden in dieser Stellungnahme auch die Erläuterungen zum VE-VEKJ geprüft und mit Hinweisen auf fehlerhafte, unhaltbare und unnötige Textstellen versehen.

3.2 Begrifflichkeit

3.2.1 Begriff «Dokument»

Papierdokumente werden im erläuternden Bericht zum VE-VEKJ als «papierne Dokumente» und im VE-VEKJ selbst als «physische» Dokumente bezeichnet. Dateien werden als elektronische Dokumente bezeichnet. Es wird angeregt, die Begriff Dateien zu verwenden, wenn von Dateien die Rede ist, und den Begriff «elektronische Dokumente» zu vermeiden. In Bezug auf Papier-Dokumente wird vorgeschlagen, eine ähnliche Begrifflichkeit wie bspw. in der EÖBV zu verwenden, die von Papierdokumenten spricht, ausser es werde im VE-VEKJ ausdrücklich ein weiterer Begriff angestrebt, der auch physische Dokumente auf Nicht-Papierträgermaterial umfasst.

Der Antrag des Regierungsrates des Kantons Bern zu Art. 4 VE-VEKJ wird unterstützt (vgl. Stellungnahme vom 17.09.2026, Ziffern 6.1 und 6.2, Seite 4/19).

3.2.2 Begriff «Organisation»

Der Begriff «Organisation» wird im VE-VEKJ im Zusammenhang mit Profilen auf der Plattform justitia.swiss verwendet. Das BEKJ verwendet den Begriff nicht und definiert ihn im vorliegenden Kontext folglich auch nicht. Die Plattform justitia.swiss hat auf der TRAIN-Instanz mit Release vom 14. April 2026 den Begriff Organisation durch den Begriff «Profil» ersetzt, vgl. die entsprechenden Release-Notes: «In diesem Release wurden auf der Plattform alle als Einzelperson registrierten Profile zu Profilen (ehemals als Organisationsprofile benannt) migriert. Jeder Nutzer, der sich als Einzelperson registriert hat, besitzt nun ein Profil, das er alleine nutzen kann. Er hat nun aber jederzeit die Möglichkeit, weitere Mitglieder in sein Profil einzuladen.» Damit einher geht offenbar die Änderung, dass neue auch Einzelpersonen-Profile eine API-Key erstellen und Berechtigungen vergeben können. Es stellt sich die Frage, ob der VE-VEKJ hier auf die alte Begrifflichkeit der Plattform justitia.swiss Bezug nimmt.

3.2.3 Begriff «Behörde»

Vgl. Bemerkungen zu Art. 4 VE-VEKJ.

3.2.4 Begriff «Benutzerinnen und Benutzer»

Der VE-VEKJ und der erläuternde Bericht verwenden dieses Begriffspaar in unterschiedlichen Kontexten, was zu Verwirrungen führt. Vgl. dazu Ziffer 4.16.1.

3.3 Ungerechtfertigte dominante Rolle von EJPD/BJ

Das EJPD ist für die Betriebsbewilligung zuständig (Art. 25 Abs. 1 BEKJ). Es ist zwar nicht unzulässig aber staatsrechtlich doch bedenklich, wenn nun das gleiche EJPD, das Bewilligungsbehörde ist, mit der Departementsverordnung nun auch noch die generell-abstrakten Regelungen erlassen darf, die es dann selber und teilweise ausschliesslich im individuell-konkreten Entscheid umsetzt. Die staatsrechtlichen Bedenken sind insbesondere auch vor dem Hintergrund der verfassungsrechtlich verankerten Unabhängigkeit der Justiz (insbesondere der Gerichte) zu sehen. Obwohl die Bundesverfassung in Art. 191c BV von einer institutionellen Unabhängigkeit der Gerichte ausgeht, die teilweise auch die Selbstverwaltung der Gerichte einschliesst, wird es hier einem Departement der Bundesverwaltung überlassen, wenn zwar technische, aber dennoch wichtige Fragen des elektronischen Rechtsverkehrs abschliessend zu regeln.

Die Subdelegation der Rechtsetzungsbefugnis zur Detailregelung des Bewilligungsverfahrens in Art. 3 Abs. 2 VE-VEKJ 3 ist zudem ohnehin nicht zulässig, sie geht über die Befugnisse des Bundesrats nach Art. 47 Abs. 1 RVOG hinaus (Details siehe dort). Das Gleiche gilt für die Rechtsetzungsdelegation in Art. 25 Abs. 1 VE-VEKJ (Details siehe dort).

Zur Departementsverordnung des EJPD muss – falls an dieser Rechtsetzungsdelegation festgehalten werden sollte – ebenfalls ein Vernehmlassungsverfahren durchgeführt werden (Art. 3 Abs. 1 Bst. e VlG).

Bei Justitia 4.0 handelt es sich grundsätzlich um ein Projekt zu eGovernment (EGOV). Dieses EGOV-Projekt könnte auch bei Bundeskanzlei angesiedelt sein bzw. bei der Digitalen Verwaltung Schweiz. Wenn man eine Subdelegation von Rechtsetzungsbefugnissen machen will, dann wäre für technische Regelungen die Bundeskanzlei geeigneter als das EJPD.

3.4 Gemeinsame Verordnung für Plattform nach Art. 6a VwVG und für Plattformen nach BEKJ wird abgelehnt

Vgl. Ziffer 4.6.1.3.

3.5 Handhabung von Rechtsetzungsdelegationen

3.5.1 Fehlende Regelungen

3.5.1.1 Regelung zu den Anforderungen an Schnittstellen fehlt

Der VE-VEKJ enthält keine Regelung zu den Anforderungen an Schnittstellen, wie dies Art. 19 Abs. 3 BEKJ vorsieht («Der Bundesrat regelt die Anforderungen an die Schnittstellen»). Art. 10 VE-VEKJ äussert sich unter den Titel «Schnittstelle» nur zur Berechtigungs-Äquivalenz («Der technische Zugang über eine Schnittstelle gilt als Berechtigung nach Artikel 24 Absatz 1 BEKJ.»).

3.5.1.2 Regelung zu den Anforderungen an Interoperabilität fehlt

Der VE-VEKJ enthält keine Regelung zu den Anforderungen die Interoperabilität, wie dies Art. 25 Abs. 3 BEKJ vorsieht: «Der Bundesrat regelt die Anforderungen an die Interoperabilität sowie das Bewilligungsverfahren und die Kostentragung.» Solche Regelungen sind unabdingbar.

3.5.1.3 Vorschlag Regelung Schnittstellen und Interoperabilität

Eine Regelung zu Schnittstellen und Interoperabilität sollte folgende Inhalte aufweisen:

- Zweck dieser Bestimmungen sollte sein, die Schnittstellen, den Datenaustausch und die Interoperabilität zwischen den Plattformen nach BEKJ, den kantonalen Plattformen sowie den mit diesen Plattformen interagierenden Fachanwendungen zu regeln.
- Es muss eine Regelung angestrebt werden, die sicherstellt, dass der elektronische Rechtsverkehr offen, sicher, transparent und nichtdiskriminierend ausgestaltet wird.
- Der Geltungsbereich der Regelungen zu Schnittstellen und Interoperabilität muss die Plattformen nach BEKJ und kantonale Plattformen ebenso umfassen wie technische Drittsysteme, die an diese Plattformen angeschlossen sind oder angeschlossen werden sollen. Der Geltungsbereich muss sowohl produktive Systeme wie auch Test- und Zertifizierungsumgebungen umfassen.
- Die Schnittstellen sind nach offenen, dokumentierten und allgemein zugänglichen Standards auszugestalten. Proprietäre Formate dürfen nur verwendet werden, wenn dies aus zwingenden Sicherheits- oder Integrationsgründen notwendig und verhältnismässig ist.
- Dokumentationspflicht: Die Betreiber der Plattformen und der technischen Drittsysteme müssen jederzeit eine vollständige und aktuelle technische Dokumentation der Schnittstellen, Datenfelder, Fehlercodes, Authentifizierungsverfahren und Versionen publizieren. Die Dokumentation ist so zu führen, dass Drittanbieter ohne Sondervereinbarungen kompatible Systeme entwickelt können. Es muss Drittanbietern beispielsweise möglich sein, Behörden auf unterschiedlichen Plattformen nach BEKJ eindeutig zu adressieren.
- Gleichbehandlung: Alle angeschlossenen Systeme und Drittsysteme müssen unter denselben technischen und organisatorischen Bedingungen Zugriff auf dieselben Funktionen und Datenqualitäten erhalten. Ungleichbehandlungen, Priorisierungen, Vergünstigungen oder Sonderzugänge sind unzulässig, sofern sie nicht durch ein formelles Gesetz begründet sind. Abrechnungsmodelle müssen die Plattformen nach BEKJ und kantonalen Plattformen leistungsgerecht gleichbehandeln.
- Versionierung und Kompatibilität: Schnittstellen sind versioniert zu führen. Änderungen mit Rückwirkung auf bestehende Integrationen sind frühzeitig anzukündigen und mit angemessenen Übergangsfristen umzusetzen. Abwärtskompatibilität ist so weit wie möglich zu gewährleisten. Der Quellcode jeder Version muss publiziert werden.
- Test- und Zertifizierungsumgebungen: Alle Betreiber von Plattformen nach BEKJ, von kantonalen Plattformen sowie von technischen Drittsystemen müssen eine nichtproduktive Testumgebung mit realitätsnahen technischen Bedingungen bereithalten. Für die Zulassung zu produktiven Schnittstellen kann eine Zertifizierung verlangt werden, deren Kriterien transparent, verhältnismässig und für alle Anbieter gleich anzuwenden sind.
- Nachweis und Protokollierung: Elektronische Übermittlungen, Abrufe, Zustellungen und Quittungen sind vollständig, strukturiert und maschinenlesbar und revisionssicher zu protokollieren. Die Protokolle müssen den Zeitpunkt, die beteiligten Systeme, den Status und die wesentlichen Identifikationsmerkmale enthalten.
- Sicherheit und Datenschutz: Die Datenübertragung hat verschlüsselt und nach anerkannten Sicherheitsstandards zu erfolgen. Es dürfen nur diejenigen Daten erhoben, verarbeitet und weitergegeben werden, die für den jeweiligen Verfahrensschritt erforderlich sind. Zugriffsrechte sind nach dem Need-to-Know-Prinzip zu gestalten.
- Aufsicht, Streitbeilegung und Weiterentwicklung: Die Betreiber der Plattformen und der technischen Drittsysteme müssen Governance-Regeln für den technischen Betrieb, die Änderung von Standards und die Behandlung von Konflikten mit angeschlossenen Systemen erarbeiten und einhalten. Streitigkeiten über technische Anschlussbedingungen, Verfügbarkeit und Gleichbehandlung sind einem geregelten Schlichtungs- oder Aufsichtsverfahren zu unterstellen.

3.5.2 Regelungen ohne oder in Überschreitung der Delegationsnorm

Die Subdelegation der Rechtsetzungsbefugnis zur Detailregelung des Bewilligungsverfahrens in Art. 3 Abs. 2 VE-VEKJ 3 ist zudem – wie bereits erwähnt – nicht zulässig, sie geht über die Befugnisse des Bundesrats gemäss Art. 47 Abs. 1 RVOG hinaus (Details siehe dort). Das Gleiche gilt für die Rechtsetzungsdelegation in Art. 25 Abs. 1 VE-VEKJ (Details siehe dort).

3.5.3 Regelung der Weiterentwicklung der Plattformen und der Departementsverordnung

Eine Departementsverordnung tritt sofort in Kraft. Die Mitwirkung aller Betroffenen muss sichergestellt sein und es muss sichergestellt sein, dass adäquate Umsetzungsfristen vorgesehen werden. Betroffen sind die Anwaltschaft, Betreiber von technischen Drittsystemen, andere Plattformbetreiber sowie die Justiz und betroffene Behörden.

3.6 Kostenfrage auf Anwaltsseite ausgeblendet

Mit dem Projekt Justitia 4.0 werden zahlreiche Tätigkeiten von den Behörden an die Anwaltschaft ausgelagert (Scannen, Erfassen von Metadaten, Dateianalysen, Bewirtschaftung von Plattformen, Anwaltskanzleien als Unterlagendrehscheiben, etc.). Das Scannen von Papierunterlagen beispielsweise ist ein aufwändiger und fehleranfälliger Prozess. Das Scannen nach TR Resiscan[1] führt zu Kosten von bis zu 90 Rappen/Seite. Es muss sichergestellt werden, dass alle auf die Anwaltschaft abgewälzten Aufwände kostendeckend abgegolten werden. Diese Frage darf nicht den kantonalen Gerichten oder Regierungen überlassen werden, sondern muss als zentraler Teil des Vorhabens Justitia 4.0 gesamtschweizerisch geregelt werden. Ansonsten führt dies, wie das nachfolgende Beispiel belegt, zu unsinnigen und für die Anwaltschaft nachteiligen Justizentscheiden: "Beim Scannen von Unterlagen ist der finanzielle Einzelaufwand im Normalfall noch deutlich geringer, da im Gegensatz zu Fotokopien keine Kosten für Papier oder Toner anfallen, so dass diese technischen Kosten vernachlässigt werden können."[2]

Deshalb muss die Abgeltung an die Anwaltschaft für solche ausgelagerten Arbeiten unmittelbar in den Prozessrechten des Bundesrechts (ZPO, StPO, BGG, etc.) geregelt werden.

3.7 Business Continuity, alternative Formen der Übermittlung im Notfall

Der Leitsatz #D6, vgl. Anhang, lautet: «Die Plattform muss über eine Notfallplanung verfügen. Im Notfall muss eine funktionierende alternative Form der elektronischen Übermittlung jederzeit zur Verfügung stehen.» Weder das BEKJ noch die vorliegende VEKJ regelt das Vorgehen für den Fall, dass die Plattform justitia.swiss (vorübergehend) nicht zur Verfügung stehen sollte oder dass der Plattform justitia.swiss oder einer anderen anerkannten nach BEKJ zugelassenen Plattform in Anwendung von Art. 25 BEKJ i.V.m. Art. 3 Abs. 4 VE-VEKJ die Betriebsbewilligung entzogen werden sollte. Das BEKJ regelt lediglich den Fall des Nichtzustandekommens der Vereinbarung gemäss Art. 3 Abs. 2 BEKJ. Im Kanton Bern jedenfalls könnte im Fall einer Nichtverfügbarkeit der Plattform justitia.swiss bzw. im Fall eines Bewilligungsentzugs nicht auf einen nicht-vertraulichen elektronischen Übermittlungsweg ausgewichen werden.

4 Kommentare zu Titel, Ingress und zu den einzelnen Artikeln

4.1 Titel der Verordnung

Das BEKJ trägt den Titel „Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz“. Die VEKJ enthält Vollzugsvorschriften zum ganzen BEKJ. Der Titel der Verordnung «Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren» ist mithin enger gefasst, nicht konzise und deshalb nicht nachvollziehbar.

---

[1] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Ersetzendes-ScannenTR-Resiscan/ersetzendes-scannentr-resiscan_node.html

[2] Entscheid RBOG 2015 Nr. 28, Barauslagen nach § 14 Anwaltstarif, https://entscheidsuche.ch/view/TG_OG_001_RBOG-2015-Nr--28_2011

Insbesondere ist zu bemerken, dass die zentrale Plattform justitia.swiss gerade nicht der elektronischen Kommunikation in der Justiz dient, sondern nur dem Austausch von Dateien in der Justiz, wie Art. 2 Abs. 2 Bst. a BEKJ richtig festhält. Dies bedeutet, dass elektronische Kommunikation ohne Dateiübermittlung nicht vom BEKJ geregelt wird und dass die elektronische Kommunikation zwischen Behörden und Behörden und zwischen Behörden und Rechtsanwält:innen und Bürger:innen über alternative Übermittlungswege stattfinden muss.

Dabei muss es sich um vertrauliche elektronische Kommunikation handeln, soweit kantonale oder bundesrechtliche Vorgaben diesbezüglich bestehen. Im Kanton Bern gehören Verfahrensakten und generell Informationen aus Straf-, Zivil-, SchKG- und Verwaltungsverfahren grundsätzlich zur Vertrauensstufe 2 (Vertraulich). Gemäss der kantonalen Weisung über den Umgang mit ICT in der Kantonsverwaltung für Endanwenderinnen und Endanwender vom 21. Oktober 2025 (Version 1.02) dürfen E-Mails mit Schutzbedarf 2 oder 3 an verwaltungsexterne Adressen nicht unverschlüsselt versendet werden.

4.2 Ingress

In den Erläuterungen zum VE-VEKJ wird ausgeführt, weshalb beim BEKJ das ganze Gesetz im Ingress erwähnt wird und nicht die einzelnen Delegationsnormen im BEKJ, auf die sich die VEKJ stützt. Dies widerspricht den Redaktionsregeln für Verordnungen des Bundesrats. Zudem wird damit verwischt, auf was sich die VEKJ im Einzelnen stützt. Bei dem ohnehin schon überlangen Ingress spielt es keine Rolle mehr, wenn auch die massgeblichen Delegationsnormen im BEKJ einzeln aufgeführt werden. Der Ingress hat mithin im Interesse der Transparenz alle Delegationsnormen in Gesetzen aufzulisten. In diesem Punkt wird auch auf die Stellungnahme des Regierungsrates des Kantons Bern vom 17.06.2026 verwiesen (Ziffern 1.1 und 1.2, Seite 2/19).

4.3 Zum Kapitel 1 «Ausgangslage» des erläuternden Berichts

Vorschlag: Der letzte Satz dieses Kapitel ist zu streichen.

Begründung:

Der Satz ist beschönigend und irreführend. Es wurden zum Zeitpunkt der Erstellung des erläuternden Berichts nur einige wenige Pilotprojekte durchgeführt und diese beschränkten sich mehrheitlich auf die Übermittlung von PDF-Dateien. Der Satz ist daher entweder zu streichen oder es sollten sowohl Scope wie auch Evaluationen der Pilotprojekte offengelegt werden und es sollte zusätzlich dargelegt werden, welche praxisrelevanten Fallkonstellation nicht pilotiert wurden.

4.4 Zum Kapitel 2.3 des erläuternden Berichts

Vorschlag: Die Begrifflichkeit im ganzen Kapitel ist mit der Begrifflichkeit im VE-VEKJ zu harmonisieren.

Begründung:

Der erläuternde Bericht erläutert in diesem Kapitel u.a. die Regelung zu «Einlagen». Dieser Begriff kommt in der VE-VEKJ aber gar vor.

4.5 Zum Kapitel 2 des erläuternden Berichts

Der zweitletzte Absatz wird ausdrücklich begrüsst. Die zusätzliche Integration von Drittsystemen ist dann sinnvoll, wenn in begründeten Fällen Kollegendoppel oder andere cc-Kopien versendet werden sollen oder wenn bei Nichterreichbarkeit der Plattformen ein geeignetes Beweismittel zur Glaubhaftmachung der Nichterreichbarkeit erstellt werden soll.

4.6 Artikel 1

4.6.1 Stellungnahme

4.6.1.1 Zu Absatz 1, Einleitungssatz

Vorschlag: «Die Bestimmungen des vorliegenden Kapitels sind auf folgende Plattformen ~~sowie auf die Verfahren, in welchen diese Plattformen zu nutzen sind,~~ anwendbar:»

Begründung:

Die VEKJ kann zwar im Umfang des 3. Abschnitts (von Art. 18 bis Art. 24) BEKJ auch Regelungen (Ausführungsbestimmungen) zu den Plattformen gemäss Art. 4 Abs. 1 BEKJ (kantonale Plattformen) haben (vgl. Art. 25 Abs. 2 BEKJ), nicht aber darüber hinausgehend. Zudem ist der Einleitungssatz im Absatz 1 insofern falsch, als das Kapitel nur auf die Plattformen anwendbar sein kann, nicht aber auf alle Verfahren, die über die Plattformen abgewickelt werden. Denn der Bundesrat kann nach den Prozessgesetzen nicht für alle Verfahren ergänzende Regelungen erlassen. Und wenn über eine kantonale Plattform Verfahren abgewickelt werden, die kantonalem Verfahrensrecht unterliegen, dann darf der Bund dazu keine Regelungen erlassen.

Beispielsweise kann der Bundesrat keine Regeln für das VRPG BE erlassen, nur weil Dateien in den Verfahren vor Verwaltungsgericht des Kantons Bern via die Plattform justitia.swiss übermittelt werden.

4.6.1.2 Zu Absatz 1 Bst. b und c

Vorschlag: Bst. b und c sind zu streichen.

Begründung:

Die VEKJ kann zwar im Umfang des 3. Abschnitts (Art. 18 bis Art. 24) BEKJ auch Regelungen (Ausführungsbestimmungen) zu den Plattformen gemäss Art. 4 Abs. 1 BEKJ (kantonale Plattformen) enthalten (vgl. Art. 25 Abs. 2 BEKJ), nicht aber darüber hinausgehend.

4.6.1.3 Zu Absatz 1 Bst. c

Vorschlag: Für die Plattform nach Art. 6a VwVG ist eine separate Verordnung zu erlassen.

Begründung:

Eine gemeinsame Verordnung für alle dem BEKJ unterstehenden Plattformen und für die zukünftige Plattform für die nichtstrittigen Verwaltungsverfahren des Bundes wird abgelehnt. Letztere Plattform ist zum jetzigen Zeitpunkt noch nicht einmal ausgeschrieben. Es wird befürchtet, dass durch diese Verknüpfung die Errungenschaften der Plattform justitia.swiss, die eine echte Digitalisierung und nicht nur eine PDFisierung der Justiz anstrebt, verwässert werden und dass sich die Fertigstellung des VEKJ dadurch unnötig verzögert.

Das Projekt Justitia 4.0 hat sich offenbar geweigert, die nichtstrittigen Verwaltungsverfahren des Bundes über die Plattform justitia.swiss laufen zu lassen. Dies spricht dafür, dass die Verfahren, die via justitia.swiss laufen, deutlich von Verfahren, die über eine Plattform nach Art. 6a VwVG laufen, unterscheiden. Deshalb dürften die Bedürfnisse der betroffenen Bundesbehörden und der Anwaltschaft in solchen Verfahren wohl anders gelagert sein als im engeren Justizbereich.

4.6.1.4 Weitere Bemerkungen zum erläuternden Bericht

Der Verordnungsgeber schreibt bereits jetzt, dass «der technische Rahmen der zukünftigen Plattform des Bundes […] aktuell noch nicht bekannt» sei und dass dieser technische Rahmen die VEKJ beeinflussen könnte: «Sollten für deren Betrieb zusätzliche Regelungen auf Verordnungsstufe nötig sein, werden diese während des Vernehmlassungsverfahrens noch erarbeitet beziehungsweise nach Inkrafttreten des VE-VEKJ über eine Revision nachträglich eingefügt.»[3] Diese Formulierung ist bemerkenswert,

a) weil hier offenbart wird, dass der «technische Rahmen» der zu bauenden Plattform für die nichtstrittigen Verwaltungsverfahren des Bundes die Verordnung formen wird, und nicht etwa umgekehrt und
b) weil die hier in die Vernehmlassung gegebene Verordnung noch während des Vernehmlassungsverfahrens verändert werden soll. Dies ist angesichts des knappen Zeitrahmens beunruhigend, soll doch voraussichtlich per 1.7.2027 das BEKJ abschliessend in Kraft gesetzt werden, wozu bekanntlich die vorgängige Inkraftsetzung der VEKJ nötig ist.

[3] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens Bern vom 13. März 2026 zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ), Seite 5/40.

Es ist unannehmbar, dass die Hauptbetroffenen der VEKJ, die Kantone und ihre Straf- und Ziviljustiz ebenso wie die Anwaltschaft sich zu geplanten Änderungen der VEKJ nicht mehr äussern sollen können. Die entsprechenden Passagen im erläuternden Bericht sind entsprechend anzupassen.

4.6.1.5 Zu Absatz 2

Vorschlag: Abs. 2 ist verständlich zu formulieren oder zu streichen.

Begründung:

Leider sind die Erläuterungen zu Art. 1 VE-VEKJ sehr dürftig, so dass nicht klar wird, was hier unter spezialgesetzlichen Plattformen verstanden wird und welche Bedeutung der Absatz 2 überhaupt hat. Falls die Bestimmung beibehalten werden sollte, ist wie beim Einleitungssatz zu bedenken, dass das 1. Kapitel VE-VEKJ (Art. 1 bis Art. 21) nur auf die Plattformen anwendbar sein kann, nicht aber auf alle Verfahren, die über die Plattformen abgewickelt werden.

4.6.1.6 Zu Absatz 3

Vorschlag: Abs. 3 ist zu streichen.

Begründung:

Der Absatz 3 ist entbehrlich: Spezialgesetzliche Regelungen bleiben immer vorbehalten (lex specialis derogat lex generalis), sofern nicht ausdrücklich etwas anderes geregelt ist. Mithin kann der Absatz 3 ersatzlos gestrichen werden.

4.7 Artikel 2

4.7.1 Stellungnahme

4.7.1.1 Zu Art. 2

Der Bundesrat ist gemäss Art. 25 Abs. 2 BEKJ nur befugt, zusätzlich zu den Anforderungen des BEKJ „die Anforderungen an die Interoperabilität sowie das Bewilligungsverfahren und die Kostentragung“ zu regeln. Die Anforderungen dürfen zudem nicht über jene des 3. Abschnitts BEKJ hinausgehen, ausser „die Anforderungen an die Interoperabilität“. Mithin schiesst Art. 2 VE-VEKJ allenfalls über die delegierten Befugnisse hinaus, indem er zusätzliche Anforderungen an die Plattformen formuliert.

Ebenfalls fällt auf, dass der Vorentwurf VEKJ die Anforderungen an die Interoperabilität nicht regelt.

4.7.1.2 Zu Art. 2 Abs. 1 Bst. b

Vorschlag: Die Dokumente auf der Plattform werden nach dem technische Standard XY (Version Z) der Bundesverwaltung oder, sofern es sich um kantonale Plattformen handelt, äquivalenter kantonaler Standards verschlüsselt; sie werden verschlüsselt übermittelt.

Begründung:

Abs. 1 Bst. b kann sich von den Zuständigkeiten her nur auf die Plattform Justitia.swiss beziehen, nicht aber auf kantonale Plattformen. Der Bund darf den Kantonen für deren Plattformen nicht einen Verschlüsselungsstandard des Bundes aufzwingen. Dafür fehlen eine verfassungsrechtliche und eine gesetzliche Grundlage.

Abs. 1 Bst. b stellt zudem eine unzulässige dynamische Verweisung auf Standards dar; es müsste explizit auf einen konkreten Standard und dessen Version verwiesen werden.

In diesem Punkt wird die Stellungnahme des Regierungsrates des Kantons Bern vom 17.06.2026 unterstützt (Ziffer 2.1 und 2.2., Seiten 2/19 und 3/19).

4.7.1.3 Zu Art. 2 Abs. 1 Bst. c

Vorschlag: Die Plattform kann bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln. Weitere technische Begrenzungen sind nicht zulässig. Die Betreiber von Plattformen müssen Rechtsanwältinnen und Rechtsanwälten auf Anfrage die Berechtigung erteilen, grössere Dateien zu übermitteln.

Alternativer Vorschlag: Art. 2 Abs. 1 Bst. c ist zu streichen.

Begründung:

Die Train-Plattform von justitia.swiss kennt zum aktuellen Zeitpunkt Grössenbegrenzungen, die sich nicht auf die Grösse von Dateien, sondern offenbar auf andere Parameter beziehen. Dies ergab ein Test des BAV im Februar/März 2026 mit einer PDF-Datei, die weniger als 2 GB aufwies. Die Fehlermeldung lautete: «Datei nicht hochgeladen. Technische Begrenzungen wurden überschritten, bitte kontaktieren Sie den Kundensupport unter support_justitia@elca-services.com. (ID: aY23BpE-jebvCxVogc8Y2QAAAEM).» Es ist deshalb ausdrücklich festzuhalten, dass weitere technische Begrenzungen nicht zulässig sind.

Eventuell ist zu prüfen, ob die technischen Begrenzungen (2GB) nicht auf Stufe Departementsverordnung festzuhalten sind.

Schliesslich ist darauf hinzuweisen, dass ein Widerspruch besteht zwischen Ziffer 2.3 des erläuternden Berichts, wo von einer Grössenbeschränkung von 2 Gigabyte pro Dokument die Rede ist, und den Erläuterungen zu Art. 2, Bst. c des Entwurfs, wo die Grösse von 2 Gigabyte als Mindestanforderung an die Plattform bezeichnet wird.

Zur Begründung des alternativen Vorschlags wird auf die Stellungnahme des Regierungsrates des Kantons Bern vom 17.06.2026 verwiesen (Ziffer 3.2, Seite 3/19).

4.7.1.4 Zu Art. 2 Abs. 1 Bst. d

Vorschlag: Art. 2 Abs. 1 Bst. d ist zu streichen

Begründung:

Es stellt sich die Frage nach dem Sinn von Abs. 1 Bst. d. Weshalb soll der Nutzer erhaltene Daten jederzeit löschen können? Zumal der Verordnungsgeber in den Erläuterungen darlegt, dass es sich bei diesem Vorgang keineswegs um eine Löschung nach BSI handelt. Die Formulierung ist ebenso überflüssig wie irreführend. Für die weitere Begründung wird auf Ziffer 4.2 der Stellungnahme des Kantons Bern vom 17.06.2026 verwiesen (Ziffer 4.2, Seite 3/19).

4.7.1.5 Vorschlag für eine Ergänzung von Art. 2 Abs. 1

Die beiden Anträge des Regierungsrates des Kantons Bern für eine Ergänzung von Art. 2 Abs. 1 werden unterstützt (vgl. Ziffer 5.1 der Stellungnahme des Kantons Bern vom 17.06.2026, Seite 3/19 und 4/19).

4.7.1.6 Zu Art. 2 Abs. 2

Vorschlag: Grundlegende Anforderungen an die Schnittstellen sind in Art. 10 VEKJ zu regeln. Vgl. die Ausführungen zu Art. 10 VE-VEKJ: «Das Eidgenössische Justiz- und Polizeidepartement (EJPD) regelt die funktionalen ~~und betrieblichen~~ Anforderungen an die Plattformen, einschliesslich der Schnittstellen nach Artikel 19 Absatz 2 ~~Absätze 1 und 2~~ BEKJ.»

Begründung:

Die Subdelegation von Rechtsetzungsbefugnissen an das EJPD ist bezüglich der funktionalen Anforderungen und der Schnittstellen zulässig, weil es sich wohl tatsächlich um technische Regelungen handelt (Art. 47 Abs. 1 RVOG). Fraglich ist, ob auch «betriebliche» Anforderungen durch das EJPD geregelt werden dürfen; das ist schwierig abzuschätzen, weil gemäss Erläuterungen erst während des Vernehmlassungsverfahrens geklärt wird, was überhaupt dazu gehört. Jedenfalls dürfte bei kantonalen Plattformen der Regelung von betrieblichen Anforderungen Grenzen gesetzt sein.

In den Erläuterungen steht, dass bei Änderung der Schnittstellen zuvor eine Konsultation mit den Plattformbetreibern stattfinden soll. Betroffen sind aber nicht und nicht vor allem die Plattformenbetreiber, sondern die Anbieter von technischen Drittsystemen (bspw. Anwaltssoftware) sowie grössere Anwaltsunternehmen, welche diese Schnittstellen nutzen; auch diese und der SAV sowie die kantonalen Anwaltsverbände müssten in der Konsultation begrüsst werden.

Das EJPD ist für die Betriebsbewilligung zuständig (Art. 25 Abs. 1 BEKJ). Es ist zwar nicht unzulässig, aber staatsrechtlich doch bedenklich, wenn nun das gleiche EJPD, das Bewilligungsbehörde ist, durch Departementsverordnung nun auch noch die generell-abstrakten Regelungen erlassen darf, die es dann ausschliesslich selber im individuell-konkreten Entscheid umsetzt.

Zur Departementsverordnung des EJPD muss ebenfalls ein Vernehmlassungsverfahren durchgeführt werden. Vgl. dazu Ziffer 3.3.

Art. 19 Abs. 1 BEKJ regelt im Übrigen nicht die Schnittstellen, sondern die Benutzeroberfläche – diesbezüglich liegt ein Redaktionsfehler vor.

4.7.1.7 Weitere Bemerkungen zum erläuternden Bericht

Die vom Verordnungsgeber in den Erläuterungen festgehaltenen Spezialfälle und die Möglichkeit, dass spezifische Nutzer auch grössere Dateien übermitteln können[4], ist ausdrücklich in der Verordnung festzuhalten. Es ist auch ausdrücklich festzuhalten, dass Rechtsanwält:innen das Recht haben, ein qualifiziertes Profil, welches die Übermittlung von grösseren Dateien erlaubt, auf Gesuch hin zu erhalten, ohne dass daran weitere Bedingungen oder Vorbehalte verknüpft werden. Ohne eine solche Regelung auf Stufe VEKJ ist die Gleichbehandlung der Nutzerinnen und Nutzer der Plattformen nicht sichergestellt und es ist zu befürchten, dass die Plattformbetreiber unterschiedliche Praktiken zur Gewährung dieser Einwilligungen durchsetzen werden. Eine einheitliche Praxis ist vor dem Hintergrund der Interoperabilität zwischen verschiedenen Plattformen ohnehin zwingend.

4.8 Artikel 3

4.8.1 Stellungnahme

4.8.1.1 Zu Abs. 1

Es ist zu prüfen, ob das EJPD die geeignete Behörde zu Erteilung von Plattformbewilligungen ist.

Art. 3 Abs. 1 klammert die VwVG-Plattform mit Blick auf das Bewilligungsverfahren explizit aus (Bst. c von Art. 1). Dadurch entsteht Rechtsunsicherheit in Bezug auf die effektiv für die VwVG-Plattform geltenden VEKJ-Bestimmungen. Gelten beispielsweise die Anforderungen von Art. 2 für die VwVG-Plattform oder nicht?

4.8.1.2 Zu Abs. 2

Vorschlag: Absatz 2 sollte den Verweis auf die zu erfüllenden Anforderungen explizit formulieren, analog zu Abs. 4 («wenn die Anforderungen nach Art. 25 BEKJ und Artikel 2 erfüllt sind»).

Begründung:

Abs. 2 verweist hinsichtlich Anforderungen auf Art. 2 VE-VEKJ, der seinerseits auf Art. 25 BEKJ verweist, der seinerseits a) auf den 3. Abschnitt BEKJ verweist (Art. 18 bis 24, Adressverzeichnis, Benutzeroberfläche und Schnittstellen, Authentifizierung der Benutzer, Ausnahmen zur Authentifizierung, Entgegennahme und Abruf von Dokumenten, zusätzliche Benachrichtigungen, Weitergabe und Verwaltung von Berechtigungen), b) Anforderungen an die Interoperabilität und c) Anforderungen betr. öffentliche Zugänglichkeit des Quellcodes formuliert.

In diesem Zusammenhang ist auch zu beobachten, dass Art. 10 VE-VEKJ sich unter den Titel «Schnittstelle» nur zu Berechtigungs-Äquivalenz äussert («Der technische Zugang über eine Schnittstelle gilt als Berechtigung nach Artikel 24 Absatz 1 BEKJ.»)

4.8.1.3 Zu Abs. 3

Vorschlag: Die Detailregelung des Bewilligungsverfahrens hat im VEKJ zu erfolgen.

Begründung:

Die Subdelegation der Rechtsetzungsbefugnis zur Detailregelung des Bewilligungsverfahrens im Absatz 3 ist nicht zulässig, sie geht über Art. 47 Abs. 1 RVOG hinaus. Im Verfahrensrecht sind das Legalitätsprinzip und die erforderliche Normhöhe strenger zu handhaben als bei den übrigen Rechtsnormen (des materiellen Rechts). Zudem wird mit dieser Rechtsetzungsdelegation die Regelungsbefugnis des EJPD bezüglich der Bewilligungen übermächtig und übermässig.

4.8.1.4 Zu Abs. 4

Vorschlag: Art. 3 ist zu ergänzen durch eine Regelung im Fall eines Entzugs der Betriebsbewilligung oder Ausfalls der Plattformen.

Begründung:

[4] Vgl. Erläuternder Bericht, Seite 11/40

Vgl. dazu auch die Erläuterung in Ziffer 3.7. Abs. 4 wurde offenbar verfasst, ohne dass man die Folgen eines Entzugs der Bewilligung bis ans Ende durchdacht hat; diesen Eindruck erhält man auch, wenn man die Erläuterungen liest. Wenn die Bewilligung entzogen ist, dann darf die betreffende Plattform nicht mehr genutzt werden. Das bedeutet, dass die an die betreffende Plattform angeschlossenen Kantone sich sofort einer anderen Plattform anschliessen müssen (wobei „sofort" insofern relativiert ist, als wohl noch Verträge geschlossen werden müssen, evtl. mit Genehmigung durch die Kantonsregierung). Es gibt dann zwei mögliche Szenarien:

a) Es gibt noch mindestens eine andere Plattform: die betroffenen Kantone können sich dort anschliessen.
b) Es gibt keine andere Plattform (das wäre wohl der „Regelfall", wenn die Plattform justitia.swiss betroffen ist), dann fehlt im BEKJ und im VE-VEKJ ein Alternativszenario.

4.8.1.5 Neuer Abs. 6

Vorschlag: Art. 3 ist zu ergänzen durch eine Regelung im Fall eines Entzugs der Betriebsbewilligung oder Ausfalls der Plattformen und mit einer Regelung, wonach Verfügungen betreffend Erteilung oder Entzug einer Betriebsbewilligung vollständig zu publizieren sind.

Begründung:

Art. 3 VE-VEKJ muss um einen Absatz 6 ergänzt werden, der verpflichtend festhält, dass die erteilten Betriebsbewilligungen sowie die Verfügungen betreffend Entzug einer Betriebsbewilligung im Bundesblatt veröffentlicht werden müssen. Die ersteilten Betriebsbewilligungen sollen unmittelbar nach Erlass und nicht erst bei Rechtskraft veröffentlicht werden, die Verfügungen über den Entzug der Betriebsbewilligung erst nach Eintritt der Rechtskraft (auch zum Schutz des betroffenen Plattform-Trägers).

Die potenziellen Nutzer/innen müssen verbindlich wissen, ob und ab wann eine Plattform über eine Betriebsbewilligung verfügt und im Sinne des BEKJ rechtmässig genutzt werden darf. Das Gleiche gilt beim Entzug der Betriebsbewilligung: Diesbezüglich müssen die Nutzer/innen klar wissen, dass und ab wann sie die betreffende Plattform nicht mehr nutzen dürfen. Da es um die Rechtsgültigkeit von Eingaben an Justizbehörden geht, muss hier rechtlich verbindliche Klarheit herrschen.

Die potentiellen Nutzer/innen müssen zudem verbindlich wissen, in welchem Umfang die Betriebsbewilligung gültig oder eben nicht mehr gültig ist. Bei den heutigen anerkannten Zustellplattformen scheint nicht einmal der Bundesverwaltung selbst so ganz klar zu sein ob PrivaSphere und IncaMail insgesamt anerkannte Plattformen sind oder nur die jeweiligen Versandart „EGOV-Einschreiben" eine anerkannte Zustellplattform darstellt (vgl. Urteil des BGer 8C_604/2024 vom 27. November, E. 6.3).

Im Fall eines Entzugs der Betriebsbewilligung wäre zudem zu regeln, wie in der Folge bereits auf der Plattform befindliche Dateien zugegriffen werden kann. Dies betrifft insbesondere Dateien, die eine Partei noch nicht abgeholt hat.

Es könnte sein, dass das EJPD einer Plattformträgerschaft eine Betriebsbewilligung erteilt, ohne dass alle (auch technischen) Voraussetzungen erfüllt sind. Dagegen müssen Konkurrenten bzw. potenzielle Konkurrenten, aber in bestimmten Fällen wohl auch die Anwaltschaft Beschwerde führen können, und zwar bevor die Plattform den Betrieb aufnehmen darf.

Allgemeines Transparenzgebot: Wenn keine Pflicht zur Veröffentlichung bzw. zur Verankerung des öffentlichen Zugangs besteht, dann besteht die Gefahr, dass das EJPD keinen Zugang zu den amtlichen Dokumenten der Betriebsbewilligung gewährt, bspw. diese mit der Begründung, das Geschäftsgeheimnis der Plattformträgerschaft werde verletzt, verweigert.

4.9 Artikel 4

4.9.1 Stellungnahme

4.9.1.1 Zu Abs. 1

Vorschlag: Der Entwurf ist zu konkretisieren und der persönliche Geltungsbereich ist explizit zu regeln.

Begründung:

Der Begriff «Dokument» wird im BEKJ als Synonym des Begriffs «Dateien» verwendet. In Absatz 1 wird der Begriff Dokumente nun aber in Abgrenzung zum Begriff Beilage verwendet, wobei damit in der Regel elektronische Beweismittel (ebenfalls Dateien) gemeint sein dürften. Es ist davon auszugehen, dass hier bei den übrigen Verfahrensparteien nur die Rechtsschriften gemeint sind. Eine mögliche Formulierung könnte lauten: Die Verfahrensleitenden und die Verfahrensbeteiligten [passender Begriff, vgl. nächster Abschnitt] erstellen ihre Rechtsschriften, Verfügungen, Urteile, Entscheide und Mitteilungen zur Übermittlung an die Plattformen im Format PDF/A, die übrigen Verfahrensbeteiligten erstellen Rechtsschriften im Format PDF oder PDF/A.

Zudem ist der Begriff «Behörde» unklar. Welche Behörden, die bspw. von Gerichten oder Staatsanwaltschaft typischerweise beauftragt werden, müssen die Plattform verwenden, um sich an Gerichte oder Staatsanwaltschaften zu wenden? Fällt im Kanton Bern das Institut für Rechtsmedizin in diesen Anwendungsbereich? Zu bemerken ist auch, dass Art. 103c nStPO den «Austausch von Dokumenten mit der Strafbehörde» umfasst (Art. 103c Pflicht zur elektronischen Übermittlung: Abs. 1 Behörden sowie berufsmässig handelnde Rechtsbeistände müssen den Austausch von Dokumenten mit der *Strafbehörde* über eine Plattform nach dem BEKJ abwickeln. Abs. 2 Der Bundesrat kann für Behörden Ausnahmen vorsehen. Art. 24 VE-VEKJ legt nun aber davon eine Abweichung fest (Übermittlung von Dokumenten unter Behörden auf anderem Weg als über eine Plattform nach BEKJ) und die Erläuterungen halten fest, dass damit auch der Rechtsverkehr mit Gerichten gemeint sei. Mithin ist nicht klar, wie diese Bestimmungen miteinander vereinbar sein sollen.

Zu Art. 103c nStPO ist auch zu bemerken, dass der VE-VEKJ keine ausführende Bestimmung zu Art. 103 d nStPO enthält. Art. 103d nStPO trägt den Titel «Elektronische Kommunikation auf Verlangen der Partei». Absatz 1 hält hingegen fest: «Ist eine Person nicht zur elektronischen Kommunikation mit der Strafbehörde verpflichtet, so kann sie verlangen, dass die Kommunikation mit ihr über eine Plattform nach dem BEKJ elektronisch abgewickelt wird. In diesem Fall muss sie auf der Plattform eine Adresse angeben.» Mithin ist nicht klar, ob juristische Personen des Privatrechts, die regelmässig mit Strafbehörden Unterlagen austauschen, die Plattform verwenden dürfen, auch wenn sie keine Parteistellung innehaben.

4.9.1.2 Zu Abs. 2

Dieser Absatz wird ausdrücklich begrüsst und wird als Absage an jeglichen Dateiformat Numerus clausus im Bereich der elektronischen Beweismittel (Beilagen) verstanden.

Der Text von Absatz 2 ist im Wortlaut klar: Beilagen können in jedem Format übermittelt werden – ohne jede Einschränkung. Es geht deshalb nicht an, über den erläuternden Bericht diese Wahlfreiheit einschränken zu wollen, indem man dort festhält, das Risiko, ob eine Behörde ein Dokument öffnen könne, liege beim, Absender oder es gehöre zur anwaltlichen Sorgfaltspflicht, zu prüfen, ob die Behörde das Dokument bearbeiten könne. Wollte man das so handhaben, dann müsste das in der Bundesratsverordnung explizit geregelt werden, wofür aber dem Bundesrat dann wohl eine geeignete Delegationsnorm fehlt. Die Sätze „Grundsätzlich liegt das Risiko […]“ bis […] „oder die empfangende Behörde die Beilage öffnen kann“ auf Seite 15/40 des erläuternden Berichts sind demnach zu streichen.

Die Bemerkung im erläuternden Bericht, wonach „immer wenn möglich und sinnvoll auch Beilagen im Format PDF oder PDF/A übermittelt werden sollen“, lässt erahnen, wie sehr der Verordnungsgeber dem rechtlich wie technisch offensichtlichen Irrweg der PDFisierung der Justiz anhängt.

4.9.1.3 Zu Abs. 3

Vorschlag: Abs. 3 ist ersatzlos zu streichen.

Begründung: Abs. 3 VE-VEKJ stellt eine unzulässige Einschränkung verfassungsmässig geschützten Anspruchs auf rechtliches Gehörs dar und öffnet Tür und Tor für einen Flickenteppich in Sachen elektronische Beweismittel, der zu Rechtsunsicherheit und erheblichem Mehraufwand auf Anwaltsseite wie auch auf Seiten der polizeilichen Ermittlung führen wird.

Abs. 3 erzwingt zudem eine Fortführung der bereits heute weit verbreiteten und problematischen Praxis, antiforensische Massnahmen[5] bei der Erstellung von Verfahrensakten durchzuführen.

Behörden und Gerichte müssen ihre Beweiswürdigung auf Basis der initial eingereichten, unveränderten elektronischen Beweismittel vornehmen. Justitia 4.0 muss zwingend mit einer Befreiung von Behörden und Gerichten aus der Zwangsjacke der Standardinformatik einhergehen.

Die Aufzählung der zwingend zu bearbeiteten Dateiformate in Abs. 3 ist willkürlich und sinnentleert. Sie umfasst nicht einmal alle Dateiformate, die mit Windows-Bordmitteln verarbeitet werden, wie etwa das Bildformat TIF(F) oder das Dateiformat .svg oder .txt. Weiter fehlt beispielsweise das Dateiformat .html, das in Strafverfahren eine wichtige Rolle spielt (bspw. Exporte von Social media-Inhalten). Zudem gibt es zahlreiche verbreitete Dateiformate wie Formate für Geoinformation (z.B. Interlis), die zwar nicht mit Windows-Bordmitteln, aber mit entsprechender Software visualisiert und analysiert werden können. Zum selben Ergebnis kommt man insbesondere auch, wenn man die Liste mit den im Bereich OGD vom Bund empfohlenen Formaten abgleicht[6].

Und wenn in den Erläuterungen steht, dass ein Kriterium auch sei, dass man das Format in Smartphones öffnen könne, dann ist das nicht sachgerecht, weil Behörden, Gerichtsschreiberinnen und Gerichtsschreiber und Richterinnen und Richter üblicherweise nicht auf Smartphones arbeiten. Weder die kantonalen GEVER-Systeme noch die JAA noch forensische Spezialsoftwares eignen sich soweit derzeit ersichtlich für eine Anwendung auf dem Smartphone.

4.9.1.4 Zu Abs. 4

Vorschlag: Abs. 4 ist ersatzlos zu streichen.

Begründung: Es wird auf die Begründung zu Abs. 3 verwiesen.

Wenn jede Behörde und jedes Gericht, wie dies der erläuternde Bericht nahelegt, eigene Merkblätter zu den Dateiformaten verfasst, die es verarbeiten kann, wird nicht nur kantonal eine Flickenteppich eröffnet, sondern es wird unter dem Titel der Digitalisierung der Justiz eine eigentliche Deharmonisierung der Rechtsanwendung in der Schweiz eingeführt.

Abs. 4 zwingt Rechtsanwältinnen und Rechtsanwälte ebenso wie Bürgerinnen und Bürger, die sich freiwillig auf Plattformen registrieren, zu unzulässigen Veränderungen von elektronischen Beweismitteln mit dem damit verbundenen Risiko, der Urkundenfälschung bezichtigt zu werden. Die Regelung in Absatz 4 verlangt von der Anwaltschaft und von einreichenden Behörden explizit die Vornahme von Handlungen, die dem objektiven Tatbestand einer Urkundenfälschung entsprechen können, denn jede Konvertierung von Beweismitteln in ein anderes Dateiformat verändert diese. Da diese Regelung nun auf Verordnungsebene erfolgt, vermag sie keinen Rechtfertigungsgrund darzustellen.

Abs. 4 führt zudem zu einer unbezahlten Auslagerung von Arbeiten im Bereich der Analyse und Würdigung von elektronischen Beweismitteln, dem Kerngeschäft von Behörden und Gerichten, an Rechtsanwält:innen. Hier ist in Erinnerung zu rufen, dass letztere das Dateiformat elektronischer Beweismittel weder festlegen noch festzulegen haben, sondern im Sinne des Prinzips der Chain of Custody Beweismittel in der initial vorliegenden Form an die Behörden und Gerichte übergeben. Behörden und Gerichte müssen im Zuge der Digitalisierung der Justiz in der Lage sein (oder versetzt werden), mit elektronischen Beweismitteln umzugehen (Wahrnehmung in geeigneter Form, Validierung, Würdigung, etc.).

Die Regelung von Absatz 4 ist gegenüber der Anwaltschaft auch unverhältnismässig, weil sie voraussetzt, dass Anwaltskanzleien in der Lage sein müssen, Dateien in jedes beliebige von einer Justizbehörde gewünschte Format zu konvertieren. Wenn schon, dann dürften Justizbehörden nur die Konvertierung in Formate nach Absatz 3 verlangen. Dies würde jedoch voraussetzen, dass die Anwaltschaft dafür bezahlt und durch ein formelles Gesetz ermächtigt würde, elektronische Beweismittel zu verändern und diese Veränderung zu dokumentieren. Weder das BEKJ noch die

[5] Definition gemäss NIST: Anti-Forensic: A technique for concealing or destroying data so that others cannot access it. https://csrc.nist.gov/glossary/term/anti_forensic, konsultiert am 08.06.2026

[6] https://www.bfs.admin.ch/bfs/de/home/dienstleistungen/ogd/dokumentation/empfohlenen-formate.html, konsultiert am 08.06.2026

einschlägigen Verfahrensgesetze sehen solche Entschädigungen vor. Dies ist ein weiterer Grund, diese Regelung abzulehnen.

Weiter stellt sich die Frage, wie sich Abs. 4 in den Rechtsmittelverfahren auswirkt: Was, wenn die Vorinstanz Beilagen in einem Format akzeptiert, welche die Rechtsmittelinstanz nicht akzeptiert oder umgekehrt. Wer würde diesfalls die elektronischen Beweismittel konvertieren und für diese Veränderungen die Verantwortung bzw. Haftung übernehmen?

Mit dieser Regelung wird gewissermassen auch der Bock zum Gärtner gemacht: Dieselben Behörden und Gerichte, die mit Abs. 3 zur Fortführung der gescheiterten PDFisierung der Justiz ermutigt werden sollen und denen die grosse Vielfalt der Dateiformate im Bereich der elektronischen Beweismittel offenbar mangels technisch-juristischen Knowhow und mangels entsprechender IT-Ausrüstung nicht zugemutet werden kann, sollen dann wiederum in Anwendung von Abs. 4 in der Lage sein, das geeignete Format festzulegen, in das eine Datei, mit der sie nicht umgehen können, konvertiert werden soll.

4.9.1.5 Zu Abs. 5

Vorschlag: Abs. 5 ist ersatzlos zu streichen.

Begründung:

Es wird auf die Begründung zu Abs. 3 und Abs. 4 verwiesen.

4.9.1.6 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag: Im zweiten Absatz ist der Begriff „archivtauglich“ zu streichen.

Begründung:

Gemäss KOST-CECO (KaD) sind nur die Ausprägungen PDF/A-1 und A-2 archivtauglich. Zur Ausprägung schreibt die KOST: «PDF/A-3 ist im Hinblick auf die Archivierung spezifiziert worden, widerspricht aber den Anforderungen an die dauerhafte Archivierung.»[7]

Vorschlag: Der Text zu Abs. 2 ist zu streichen oder nach Konsultation des heutigen Stands der Wissenschaft i.S. elektronische Beweismittel zu überarbeiten.

Begründung:

Es trifft nicht zu, dass für elektronische Beweismittel («Beilage») das Format PDF am tauglichsten sei. Elektronische Beweismittel liegen originär regelmässig in anderen Dateiformaten als PDF/A vor. Bei diesen Dateien stellt die Konvertierung in ein PDF-A-Format eine antiforensische Massnahme dar. Es erstaunt, dass das Bundesamt für Justiz antiforensische Massnahmen als geeignet erachtet, die Digitalisierung der Justiz in der Schweiz voranzubringen. Es sei in diesem Kontext auf die einschlägigen internationalen Standards verwiesen:

- ISO/IEC 27037:2012(E) behandelt die Themen «Information technology, Security techniques, Guidelines for identification, collection, acquisition, and preservation of digital evidence».
- ISO/TR 15801:2017 ergänzt den ISO-Standard 27037:2012, er behandelt die Themen «Document management, Electronically stored information, Recommendations for trustworthiness and reliability».
- ISO/IEC 27042:2015 ergänzt den ISO-Standard 27037:2012, er behandelt die Themen «Information technology, Security techniques, Guidelines für the analysis and interpretation of digital evidence».

Vorschlag: Der Text zum Kapitel „Verworfene Variante: Nachfordern des Originalformats“ ist ab „Zudem kann“ bis zum Schluss des Absatzes zu streichen

Begründung:

Es trifft nicht zu, dass bei einer Konvertierung in ein Dokument im PDF nur der sichtbare Teil in das PDF-Dokument übertragen wird. Diese Behauptung ist technisch offensichtlich falsch. Ebenso unzutreffend ist die Behauptung, dass PDF-Dokumente grundsätzlich wieder in die Originalformate

[7] https://kost-ceco.ch/cms/pdf-a-3.html, konsultiert am 07.06.2026

zurückkonvertiert werden könnten. Abgesehen davon, dass der Begriff «Originalformate» unglücklich ist, ist das beschriebene Prozedere technisch unmöglich: Wenn eine Worddatei mit dem SHA-256-Wert 3484dee709cd24f0aa82cc55d8ba12e65b04ab21bbfb0a83529019b1ee585236 in eine PDF-Datei konvertiert wird, lässt sich aus dieser PDF-Datei die Word-Datei mit diesem Hashwert nicht erzeugen.

4.10 Artikel 5

4.10.1 Stellungnahme

4.10.1.1 Neuer Absatz 1

Es wäre sinnvoll, wenn die VEKJ die Rechtsnatur der Quittung explizit regeln würde: Handelt es sich um eine Gültigkeitserfordernis für Eingaben oder ist es eine bloss beweisrechtliche Ordnungsvorschrift? Das Bundesgericht hat aus der analogen Bestimmung im alten Recht eine strikte Gültigkeitsvorschrift abgleitet. Damit ist ausgeschlossen, dass bei Fehlen der Quittung die Rechtzeitigkeit auf andere Weise bewiesen wird (vgl. BGer 8C_174/2025 und BGer 8C_604/2024).

4.10.1.2 Zu Absatz 2 Bst. d Ziff. 2

Vorschlag: die Liste der aufgrund des Resultats der Virenprüfung nicht übermittelten Dokumente, deren Dateiname und *Hashwerte, wenn möglich gebildet mit zwei verschiedenen kryptografischen Hashfunktionen,* sowie deren Grösse,

Begründung:

Dateiname und Grösse einer Datei erlauben es nicht, eine Datei eindeutig zu identifizieren. Eine eindeutige Identifikation ist nur mittels Hashwerten möglich. Der Kriterienkatalog Zustellplattformen vom 16. September 2014 sieht die Verwendung von zwei Hashwerten mit verschiedenen kryptografischen Hashfunktionen vor. An dieser sinnvollen Lösung ist hier festzuhalten. In der Departementsverordnung ist zudem festzuhalten, in welchem Rhythmus der Verordnungsgeber beurteilen muss, ob die aktuellen Hash-Funktionen noch adäquat sind, oder ob mindestens eine neue kryptografische Hashfunktion eingesetzt werden soll.

Problematisch ist bei Absatz 2 generell, dass „Übermittlung“ kein Zeitpunkt sondern Zeitraum ist. Erst aus dem erläuternden Bericht wird klar, dass der Zeitpunkt des erfolgreichen Abschlusses der Übermittlung gemeint ist. Art. 22 Abs. 4 Bst. a lässt hingegen Raum für andere Interpretationen z.B. Beginn des Übermittlungsvorgangs („sobald die Absenderin oder der Absender ein Dokument übermittelt“).

4.10.1.3 Zu Absatz 2 Bst. g

Die Quittung nach Art. 5 Abs. 2 Bst. g erhält als einzige keinen Namen, was zu terminologischen Verwirrungen führen wird.

4.10.1.4 Zu den Absätzen 3-5

Die Absätze 3-5 sind in sich widersprüchlich bzw. überhaupt nicht zu Ende durchdacht. Das Format PDF/A ist nicht maschinenlesbar; somit sind – wie in den Erläuterungen vermerkt – in der Regel immer zwei Quittungen parallel erforderlich. Somit stimmt der Inhalt von Absatz 4 nicht. Generell wird vorgeschlagen, den Begriff «maschinenlesbar» durch den Begriff «strukturierte Daten» zu ersetzen. Falls am Konzept der doppelten Quittungen festgehalten werden soll, ist zu regeln, welche Quittung im Fall von Abweichungen gilt. Auch scheint es nicht besonders praktikabel, dass man immer parallel mit zwei Quittungen für dieselbe Tatsache hantieren muss. Dier Erläuterungen dazu sagen zwar: „Diese beiden Anforderungen lassen sich nur schwerlich in einer einzigen Quittung verwirklichen.“ Vorzuziehen wäre aber ein Dateiformat, dass gleichzeitig strukturierten Daten und für den Menschen lesbare Form aufweist (bspw. PDF-Datei mit integrierter json- oder xml-Datei).

4.10.1.5 Zu Absatz 4

Vorschlag: Die Plattformen erstellen die Quittungen im Format PDF/A. Die von Maschinen lesbaren Quittungen ~~können~~ müssen in einem anderen Format erstellt werden.

Begründung:

PDF/A-Dateien sind per se nicht maschinenlesbar, für maschinenlesbare Quittungen sind zwingend strukturierte Formate wie bspw. xml oder json vorzusehen.

4.10.1.6 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag: Der Absatz «Erkennt die Virenprüfung…» zu Abs. 2 ist wie folgt zu ändern:

«Erkennt die Prüfung auf Schadsoftware ~~Virenprüfung~~, dass ein oder mehrere Dokumente Schadsoftware enthalten, dann werden diese Dokumente nicht an die Adressatinnen und Adressaten übermittelt (vergleiche Artikel 14 Absatz 5). Jedoch werden diese Dokumente trotzdem auf der Quittung aufgeführt, *ebenfalls mit Namen und Grösse des Dokuments sowie dessen Hashwert.* ~~Auf den Hashwert kann verzichtet werden, da diese Dokumente nicht übermittelt und somit auch nicht auf Integrität geprüft werden können.»~~

Begründung:

Gerade bei nicht übermittelten Dateien ist es von besonderer Bedeutung, in einer Quittung auch den Hashwert zu dokumentieren, damit allfällige false positives der Virenprüfung nachträglich eindeutig identifiziert werden können und damit sichergestellt ist, dass beweismässig erstellt werden kann, dass eine bestimmte, eindeutig identifizierbare Datei fristwahrend einzureichen versucht wurde.

Zum zu ersetzenden Begriff «Virenprüfung» wird auf die Stellungnahme des Regierungsrates des Kantons Bern von 17.09.2026, Ziffer 15.1.1 und 15.1.2, Seite 9/19 und Seite 10/10, verwiesen.

4.11 Artikel 6

4.11.1 Stellungnahme

Vorschlag: Der Artikel ist in verständlicher und fachlich nachvollziehbarer Art und Weise neu zu formulieren. Der Begriff Siegelung (Art. 6 und Art. 7) ist aus dem Titel zu entfernen und durch einen Begriff ersetzen, der weniger Anlass zu Verwechslung gibt.

Begründung:

Der Wortlaut von Art. 6 VE-VEKJ widerspricht Art. 22 Abs. 2 BEKJ und dem Text in den Erläuterungen und ist sachlich falsch bzw. nicht nachvollziehbar.

Anzumerken ist auch, dass gewisse Dateien von Behörden eine eigenhändige Unterschrift bzw. eine QES der Autorenschaft tragen müssen, wenn wie etwa bei sachverständigen Gutachten erheblich ist, wer das Gutachten erstellt hat. Diesfalls sind QES unabdingbar, auch wenn die Kommentierung in der Botschaft zum BEKJ, BBL 2023 679 ff, S. 30, diesbezüglich das Gegenteil insinuiert.

Weiter erlauben wir uns den Hinweis, dass, sollte sich der Wortlaut von Art. 6 auf sämtliche Behörden beziehen, der Kreis der Behörden, die Dateien vor der Übermittlung an eine Plattform zu siegeln haben, sehr gross werden könnte. Bspw. die Steuerverwaltung oder Konkursämter, wenn sie Gerichten oder Staatsanwaltschaften Auskünfte erteilen.

Ferner ist zu definieren, was «zusammen übermitteln» genau bedeuten soll. Ist damit gemeint, dass eine Übermittlung aus mehreren Dateien besteht oder dass mehrere Dateien gemerged versendet werden? Wie wäre im ersten Fall sichergestellt, dass nach dem Download der Dateien der Status «zusammen übermittelt» beweismässig nachvollziehbar gemacht werden kann? Wird in einer nicht gesiegelten Datei auf die gesiegelte Datei verwiesen (Angabe des Hashwerts?) Diese Frage ist immer dann von Bedeutung, wenn der Adressat oder die Adressatin in der Lage sein muss, zu beweisen, dass eine bestimmte Datei effektiv von einer Behörde stammt.

Weiter ist im erläuternden Bericht der Absatz «Die Plattformen müssen prüfen…» zu streichen. Die Plattformen können nicht wissen, welche erforderlichen Siegel und Zeitstempel eine Behörde anzubringen hat, bspw. wenn eine Datei eine eigenhändige Unterschrift bzw. eine QES der Autorenschaft tragen muss.

Der Begriff Siegelung wird in Artikel 248 StPO in einem spezifischen, aber völlig anderen Kontext verwendet, ebenso bspw. in Artikel 552 ZGB (Siegelung der Erbschaft). Das elektronische Siegel ist eine Form der elektronischen Signatur, vgl. Art. 2 Bst. d ZertES. Es sollte deshalb der Begriff Signieren verwendet werden.

4.12 Artikel 7

4.12.1 Stellungnahme

4.12.1.1 Abs. 1 und 2

Vorschlag:

Änderung des Begriffs Siegelung im Titel, vgl. Stellungnahme zu Art. 6 VE-VEKJ.

~~Werden mehrere Dokumente zusammen übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an.~~ *Die Plattform bringt das Siegel und den Zeitstempel einem separaten Dokument an.* Das Dokument muss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.

Begründung:

Abs. 1 scheint zu insinuieren, dass einzelne Dateien direkt mit einer attached-Signatur versehen werden sollen. Dieses Vorgehen verändert die Dateien, was mit dem Prinzip der Chain of Custody nicht vereinbar ist. Die Plattform darf Dateien nicht verändern und wird dazu technisch auch nicht in der Lage sein. Sinnvollerweise wird unabhängig von der Anzahl der übermittelten Dateien immer entweder eine detached-Signatur angebracht oder ein von der Plattform zu signierendes Begleitdokument gemäss Abs. 1 erstellt, das die Hashwerte der Dateien enthält.

Betrachtet man Art. 5 und Art. 7 zusammen, so ist nicht klar, ob es sich bei den Quittungen gemäss Art. 5 um dieselben Dateien handelt wie beim «separaten Dokument» gemäss Art. 7.

Im Gegensatz zu Art. 5, der die Ausstellung von Quittungen für Dateien regelt, welche die Virenprüfung nicht «bestanden» haben, fehlt in Art. 5 und Art. 7 eine Regelung für Dateien, die aus anderen technischen Gründen nicht auf die Plattform übermittelt werden konnten. Es ist zwingend notwendig, dass die Plattformen diesfalls zur Erstellung eines entsprechenden Beweismittels verpflichtet werden, das die Fehlermeldung, die Hashwerte der nicht übermittelbaren Datei sowie deren Name und Grösse auflistet.

4.12.1.2 Weitere Bemerkungen zum erläuternden Bericht

Im erläuternden Bericht ist die Rede davon, dass seitens der Anwaltschaft das Bedürfnis bestehe, dass die übermittelten Dokumente von den Plattformen nicht geändert werden. Dazu ist festzuhalten, dass die Nicht-Veränderung von Dateien, die via die Plattformen übermittelt werden, eine Grundanforderung an eine digitalisierte Justiz darstellt, die vermutlich von allen Akteuren geteilt wird. Es handelt sich also keineswegs ein Sonderwunsch seitens der Anwaltschaft. Der Satz ist entsprechend zu streichen oder umzuformulieren.

4.13 Artikel 8

4.13.1 Stellungnahme

4.13.1.1 Zu Absatz 1

Es wird vorgeschlagen, die Authentifizierungsqualitätsstufe in der Departementsverordnung zu regeln. Dabei ist sicherzustellen, dass mindestens alle vier aktuell verfügbaren AGOV-Identitätsprüfungsverfahren, also Adressverifikation, Brief mit ID-Check (Post), Schalteridentifikation (AGOV counter) und ID/Pass-Verifikation online[8] zum Einsatz kommen können.

4.13.1.2 Zu Absatz 2

Nicht nur die Authentifizierungsqualität sollte hier eine Rolle spielen, sondern auch die Verfügbarkeit von und die Einflussnahme von Drittstaaten auf allfällige «andere Authentifizierungsdienste».

4.13.1.3 Zu Absatz 3

Der Begriff „Mitglieder einer Behörde“ bezieht sich nicht auf alle bei einer Justizbehörde angestellten und tätigen Personen, sondern nur auf die Magistraten (Richter, Staatsanwälte, Friedensrichter oder

[8] Vgl. https://help.agov.ch/?c=identcheck&l=de, konsultiert am 24.05.2026

Leiter von Schlichtungsstellen)[9]. Dem erläuternden Bericht lässt sich aber entnehmen, dass Absatz 3 es «kleinen Behörden» erlauben soll, dauerhaft das Web-Login der Plattform zu benutzen. Es ist zu vermuten, dass ein solcher manueller Upload und Download von Dateien auf die Plattformen nicht nur von «Mitgliedern von Behörden» ausgeführt wird, sondern insbesondere auch von Angestellten, die nicht zum Kreis der Mitglieder einer Behörde fallen.

Absatz 3 ist im Sinne der Interoperabilität unter den Plattformen dahingehend zu ergänzen, dass die Betreiber von Plattformen die Entscheide anderer Betreiber hinsichtlich Akzeptanz weiterer IDPs zu übernehmen haben. Der letzte Satz zu Absatz 3 im erläuternden Bericht ist in diesem Sinne zu präzisieren.

Weiter wird der Antrag gemäss Ziffer 10.1 (Seite 7/19) der Stellungnahme des Regierungsrates des Kantons Bern unterstützt. Für die Begründung wird auf Ziffer 10.2 ebendort verwiesen.

4.13.1.4 Weitere Bemerkungen zum erläuternden Bericht

Auf Seite 20/40 des erläuternden Berichts heisst es in Absatz 1 zu Absatz 1 VE-VEKJ: […] «Es ist vorgesehen, nur die Authentifizierung mittels des Authentifizierungsdienstes der Schweizer Behörden (AGOV) zu zulassen. Artikel 20 Absatz 2 BEKJ sieht vor, dass der Bundesrat bestimmt, welche elektronischen Identitätsnachweise eingesetzt werden können. AGOV erfüllt diese Voraussetzung, da […]. Es ist unklar, auf welche Voraussetzung sich die nachfolgenden Äusserungen bezieht. Art. 20 Abs. 2 BEKJ statuiert keine Voraussetzung(en), die der Bundesrat bei der Auswahl der elektronischen Identitätsnachweise zu berücksichtigen hat.

4.14 Artikel 9

4.14.1 Stellungnahme

4.14.1.1 Abs. 1

Die Regelung gemäss Absatz 1 entspricht einer zentralen Forderung der Anwaltschaft und wird begrüsst. Unklar ist in diesem Kontext aber nach wie vor, wie Falschzustellungen von Behörden an die Anwaltschaft (und an Privatpersonen) vermieden werden können, insbesondere dann, wenn ein Verfahren von einer Behörde in Gang gesetzt wird. Dem erläuternden Bericht ist zwar zu entnehmen, dass die Angabe von Vorname, Name, Postadresse und Geburtsdatum und allenfalls Organisations-Bezeichnung oder Kanzleibezeichnung ausreiche: «Mit diesen Angaben kann eine Falschzustellung faktisch ausgeschlossen werden.» (Seite 22/40, Absätze 3 und 4). Dieser Optimismus wird seitens BAV nicht geteilt. Technisch sind Falschzustellungen nicht ausgeschlossen, ein Flüchtigkeitsfehler genügt, um eine Falschzustellung auszulösen. Deshalb sollten in dieser Verordnung Falschzustellungen an ein Profil eines übrigen Benutzers oder einer übrigen Benutzerin in geeigneter Art und Weise geregelt werden, beispielsweise in einem neuen Absatz 5. Vgl. dazu die Ausführungen in Ziffer 4.14.1.3.

4.14.1.2 Abs. 3 Bst. b, Abs. 4

Vgl. Ausführungen in Ziffer 3.1.1.2.

4.14.1.3 Neuer Absatz 5

In einem neuen Absatz 5 ist festzulegen, wie die Behörden Zustellungen vornehmen müssen, wenn ein Benutzer über mehrere Profile verfügt. Dies ist insbesondere dann nötig, wenn ein Verfahren durch eine Behörde oder durch andere Benutzer der Plattform oder Dritte auf dem Papierweg initialisiert wird. Weiter ist festzulegen, wie nach Falschzustellungen vorzugehen ist und wie der Benutzer den Wechsel auf ein anderes Profil erwirken kann.

4.14.1.4 Weitere Bemerkungen

Die Anträge des Regierungsrates des Kantons Bern vom 17.06.2026 zu Art. 9 werden unterstützt (Ziffer 11.1, Seite 7/19), für die Begründung wird auf Ziffer 11.2 ebendort verwiesen.

---

[9] Vgl. bspw. Art. 170 StPO, wo zwischen Mitgliedern von Behörden und deren Hilfspersonen unterschieden wird sowie die Unterscheidung zwischen Gerichtsmitgliedern und Gerichtsschreibern auf https://www.bger.ch/index/federal/federal-inherit-template/federal-richter.htm

4.15 Artikel 10

4.15.1 Stellungnahme

Vorschlag: Art. 10 soll substanzielle Regelungen zur Interoperabilität und zu den Schnittstellen enthalten. Soweit möglich und nötig sind Details in der Departementsverordnung zu regeln. Die vorgeschlagene Regelung sollte dahingehend ergänzt werden, dass dies nur für den technischen Zugang über eine Schnittstelle gilt, die zuvor seitens Justitia 4.0-Projekt bzw. Plattformbetreiber ein Sicherheits-Assessment durchlaufen hat: Der technische Zugang über eine Schnittstelle*, der zuvor ein Sicherheits-Assessment erfolgreich durchlaufen hat,* gilt als Berechtigung nach Artikel 24 Absatz 1 BEKJ.

Begründung:

Art. 10 hat, wie bereits erwähnt, einige Grundsätze zu den technischen Schnittstellen zu regeln. Vgl. dazu die Ausführungen in Ziff. 3.5.1.3.

Die vorgeschlagene Regelung wird aus Cybersecurity-Gründen als riskant betrachtet. Es müsste wohl vorgängig ein Sicherheits-Assessment durchgeführt werden. Offenbar ist hier jedenfalls für die Plattform justitia.swiss eine OAuth2-Lösung vorgehen (technischer API-User und API-secret), die Man in the Middle-Attacken kaum verhindern kann: Wenn ein Angreifer ein (bearer) Token abfängt, kann er sich bis zum Ablauf des Tokens als der Client ausgeben. Es wäre zu prüfen, ob nicht bspw. eine Client-Certificate-Authentication implementiert werden müsste, da diese nicht auf «shared secrets» beruht.

Im erläuternden Bericht zum VE-VEKJ wird festgehalten: «Änderungen am technischen Rahmen für die Schnittstellen sowie andere Änderungen am VE-VEKJ werden in Abstimmung mit allen Betreiberinnen von Plattformen nach dem BEKJ erfolgen (beispielsweise durch eine informelle Konsultation). Betroffen sind aber nicht und nicht vor allem die Plattformenbetreiber, sondern die Anbieter von Anwaltssoftware und Anwaltskanzleien, welche diese Schnittstellen direkt nutzen sowie weitere Drittanbieter; auch diese und interessierte Anwaltskreise müssten in der Konsultation begrüsst werden.

Der erläuternde Bericht führt aus, dass die API-Tokens regelmässig bestätigt werden müssen, ansonsten diese automatisch gelöscht oder gesperrt werden. Diese Regelung ist im Zusammenhang mit der Fristwahrung von grosser praktischer Bedeutung für die Anwaltschaft. Es genügt deshalb nicht, diesen Vorgang, der dazu führen kann, dass Eingaben nicht innert Frist eingereicht werden können, im erläuternden Bericht festzuhalten. In Art. 10 ist die entsprechende Regelung – auch zum Schutz der Plattformbetreiber – festzuhalten. Insbesondere ist festzuhalten, wer von der bevorstehenden Löschung oder Sperrung von wem, wie und mit wieviel Vorlaufzeit informiert werden muss.

4.16 Artikel 11

4.16.1 Stellungnahme

4.16.1.1 Abs. 1

Vorschlag zu Abs. 1: Die Plattformen fordern ihre Benutzerinnen und Benutzer mindestens einmal pro Jahr auf, die von ihnen erteilten Berechtigungen zu bestätigen. *Die Aufforderungen sind nach den Vorgaben von Art. 22 BEKJ zu übermitteln.*

Begründung:

Der Entzug von Berechtigungen ist aus Anwaltssicht von erheblicher praktischer Bedeutung. Werden Berechtigungen kurz vor einem Fristablauf entzogen und hat der Benutzer oder die Benutzerin keine Kenntnis der Aufforderung, besteht die Gefahr, dass Fristen nicht eingehalten werden können. Die Aufforderung hat demnach so zu erfolgen, dass die effektive Übermittlung an die Benutzerinnen und Benutzer ebenso sichergestellt und mit Quittungen ausgewiesen ist, wie dies bei der Übermittlung von Dateien von Behörden an übrige Benutzerinnen und Benutzer vorgesehen ist.

4.16.1.2 Abs. 2

Vorschlag zu Abs. 2: Nicht bestätigte Berechtigungen werden drei Monate nach der Aufforderung automatisch entzogen. ~~Die betroffenen Benutzerinnen und Benutzer werden darüber informiert.~~ *Die von den entzogenen Berechtigungen betroffenen Personen und die Benutzerinnen und Benutzer werden darüber informiert.*

Begründung:

Der erläuternde Bericht führt auf Seite 23/40 im ersten Absatz zu Art. 11 aus, das Berechtigungssystem erlaube einem Benutzer oder einer Benutzerin Drittpersonen die Erlaubnis zu erteilen, im Namen der Benutzerin oder des Benutzers Eingaben zu tätigen und Zustellungen entgegenzunehmen. Dabei wird auf Art. 24 BEKJ verwiesen. Nach dieser Formulierung sind die *berechtigten* Personen Drittpersonen und die Benutzer oder Benutzerinnen sind die *berechtigungserteilenden* Personen. In diesem Sinne wäre Abs. 1 so zu verstehen, dass nur die berechtigungserteilenden Personen (= «Benutzerinnen und Benutzer») aufgefordert würden, die von ihnen erteilten Berechtigungen zu bestätigen. Abs. 2 führt in Abweichung zu dieser Begrifflichkeit dann aber neu den Begriff «betroffene Benutzerinnen und Benutzer» ein, bei denen es sich offenbar um Drittpersonen handeln soll, die Berechtigungen erhalten haben. Die neu vorgeschlagene Formulierung stellt sicher, dass diese beiden Personengruppen klar unterschieden werden und dass klargestellt ist, dass beide Personengruppen über die entzogenen Berechtigungen informiert werden.

4.16.1.3 Weitere Bemerkungen zum erläuternden Bericht

Der erläuternde Bericht bekräftigt auf Seite 23/40 den Inhalt von Art. 24 Abs. 1 BEKJ: «Mit dem Berechtigungssystem kann eine Benutzerin oder ein Benutzer Drittpersonen die Erlaubnis erteilen, im Namen der Benutzerin oder des Benutzers Eingaben zu tätigen und Zustellungen entgegenzunehmen (vgl. Art. 24 BEKJ).» Nun weist aber die Plattform justitia.swiss (PROD) weitergehende Berechtigungsmuster auf, die auf einen Anforderungskatalog aus der Anwaltschaft zurückgehen. Es wäre sinnvoll, im erläuternden Bericht klarzustellen, dass mit Art. 11 Abs. 1 nicht nur die Berechtigungen nach Art. 24 Abs. 1 BEKJ gemeint sind, sondern dass diese Regelung auf für Berechtigungen gilt, die über Art. 24 Abs. 1 BEKJ hinausgehen.

4.17 Artikel 12

4.17.1 Stellungnahme

4.17.1.1 Abs. 1

Vorschlag: Die auf einer Plattform gespeicherten Dokumente und Quittungen werden sechs Monate nach der Entgegennahme beziehungsweise nach der Erstellung automatisch ~~vernichtet~~ *gelöscht*.

Begründung:

Die minimale Aufbewahrungsdauer ist in Art. 22 Abs. 5 BEKJ mit 90 Tagen angegeben; hier wird nun die maximale Aufbewahrungsfrist mit 6 Monaten festgelegt. Es ist unschön, dass die Zeitdauer einmal in Monaten und einmal in Tagen angegeben ist.

Unklar ist, weshalb wird hier terminologisch von „vernichtet“ gesprochen wird, wenn doch elektronische Dokumente nur gelöscht werden können und „löschen“ in diesem Kontext der übliche Begriff ist, vgl. Art. 22 Abs. 5 BEKJ: «Die Dokumente und Quittungen werden frühestens 90 Tage nach der Übermittlung gelöscht. […]».

4.17.1.2 Abs. 2

Vorschlag: Stehen Dokumente zur Akteneinsicht zur Verfügung, so bestimmt die verfahrensleitende Behörde, wie lange die *einzelnen* Dokumente auf der Plattform abrufbar sind. Nach Ablauf der Frist werden die Dokumente automatisch ~~vernichtet~~ gelöscht.

Begründung:

Zum Begriff «vernichten» vgl. Ziffer 4.17.1.1.

Eine Akteneinsicht kann stufenweise erfolgen, nicht immer wird eine ganze Verfahrensakte zur Verfügung gestellt. Es kommt vor, dass nachträglich weitere Dateien einer bestehenden Akteneinsicht hinzugefügt werden, beispielsweise Rohdaten. Aus diesem Grund scheint es sinnvoll zu präzisieren, dass sich die Frist auf einzelne Dokumente (also Dateien) beziehen muss.

4.17.1.3 Weitere Bemerkungen

Der Antrag des Regierungsrates des Kantons Bern zu Art. 12 gemäss Stellungnahme vom 17.06.2026, Ziffer 13.1, Seite 8/19 und 9/19, wird unterstützt. Für die Begründung wird auf Ziffer 13.2 ebendort verwiesen.

4.17.1.4 Bemerkungen zum erläuternden Bericht

Es ist nicht hilfreich, wenn der erläuternde Bericht zu Absatz 2 in Abweichung zum Wortlaut des VE-VEKJ hier den Begriff Dokumente meidet und stattdessen von «Akten» spricht. Der Begriff «Akten» könnte als unscharfer Sammelbegriff für mehrere Dokumente verstanden werden, was in diesem Kontext nicht sinnvoll erscheint.

4.18 Artikel 13

4.18.1 Stellungnahme

Vorschlag: Der Artikel ist ersatzlos zu streichen.

Begründung:

Art. 28 Abs. 3 BEKJ ermächtigt zwar den Bundesrat, die Anforderungen an die Datensicherheit zu regeln. Es ist aber zu bezweifeln, dass er durch Verordnungsrecht den Geltungsbereich des ISG verändern darf. Gemäss Art. 3 Abs. 1 Bst. a ISG gelten die Bestimmungen des 3. Abschnitts des ISG für die Kantone, wenn sie auf Informatikmittel des Bundes zugreifen. Das ist bei Plattformen nach Art. 4 Abs. 1 BEKJ wohl der Fall, da diese Schnittstellen zumindest zu den Informatikmitteln der Gerichte des Bundes aufweisen. Somit kommt der 3. Abschnitt des ISG eo ipso für diese Plattformen zur Anwendung. Gemäss Art. 3 Abs. 2 ISG kommt das ISG allerdings nicht zur Anwendung, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten. Der Art. 13 Abs. 1 VE-VEKJ kann (bzw. muss) somit ersatzlos gestrichen werden.

Die Verweisung auf Art. 8 DSG ist zudem nicht zielführend. Es wäre sinnvoller, direkt auf die DSV zu verweisen, die der Bundesrat gestützt auf Art. 8 Abs. 3 DSG erlassen hat.

4.19 Artikel 14

4.19.1 Stellungnahme

4.19.1.1 Abs. 1 und 2

Diese Details sollten in der Departementsverordnung geregelt werden. Dabei ist prüfen, ob Virencode, der durch die Aufteilung «zerschnitten» wird, erkannt werden kann.

4.19.1.2 Abs. 2

Die Aussage von Abs. 2 als Kann-Bestimmung ist unklar: Geht es nur um eine Ermächtigung der Plattform die Dokumente aufzuteilen? Oder besagt die Bestimmung auch, dass die Plattform bei grösseren Dateien, auch ohne Ersuchen der Benutzer (Abs. 3), auf die Virenprüfung verzichten und nach Abs. 4 vorgehen kann?

4.19.1.3 Abs. 3

Diese Kann-Bestimmung ist so zu handhaben, dass Gesuche von Rechtsanwältinnen und Rechtsanwälten in der Regel gutzuheissen sind. Dies ist in den Erläuterungen festzuhalten.

4.19.1.4 Abs. 4

Es ist davon auszugehen, dass diese Dateien zusätzlich in einen ZIP-Container verpackt werden und dass der Befund auf der Quittung ausgewiesen wird. Dies ist in den Erläuterungen entsprechend festzuhalten.

4.19.1.5 Abs. 5

Hier stellt sich die Frage, ob diese Information zusätzlich zur Eingangsquittung gemäss Art. 5 Abs. 2 Bst. d Ziff. 2 VE-VEKJ erfolgen soll.

Problematisch ist bei Absatz 5, dass der Absender das Risiko für die Dauer der Virenprüfung trägt, obwohl er diese nicht kontrolliert und darauf auch keinen Einfluss hat.

4.19.1.6 Weitere Bemerkungen

Die Anträge 1 bis 3 des Regierungsrates des Kantons Bern zu Art. 14 werden unterstützt, vgl. Stellungnahme vom 17.06.2026 Ziffern 15.1.1 bis 15.3.2, Seiten 9/19 und 10/19.

4.20 Artikel 15 bis 21

4.20.1 Stellungnahme

Weitere Plattformen sollten nach derselben Gebührenlogik behandelt werden müssen, dies ist in der Verordnung entsprechend zu ergänzen.

Art. 15 Abs. 1: Der Absatz 1 ist verwirrend formuliert. Gemeint ist hier wohl nicht die «Gesamthöhe der Gebühr», sondern die Summe der Gebühreneinnahmen. Hier von einer Gesamtgebühr auszugehen, die dann aufgeteilt wird, ist seltsam; auch Art. 32 BEKJ spricht von «Gebühren».

Art. 17 Abs. 3: Der Absatz 3 ist entbehrlich. Diese Aufteilung vornehmen könnte jedes Departement auch ohne Regelung in der VEKJ. In den Erläuterungen steht – bezogen auf die Absätze 2 und 3 – dass damit dem «Verursacherprinzip» Rechnung getragen werden könne. Das ist nicht einleuchtend. Denn erstens kommt das Verursacherprinzip nur im Subordinationsverhältnis zwischen Staat und Privaten zum Tragen. Und zweitens hat der proportionale Anteil von Justizfällen eines Departements oder Amts sachlich nichts mit dem Verursacherprinzip zu tun: Die Bundesstellen können in keiner Weise steuern, wie viele Verfügungen sie erlassen müssen und welcher Anteil davon mit Beschwerde angefochten wird. Zudem kommt die Plattform nur für Justizverfahren (nicht für reine Verwaltungsverfahren) zur Anwendung und die Kosten von Beschwerdeverfahren fallen zum grössten Teil beim Bundesverwaltungsgericht an.

Art. 18: Gemäss Art. 32 Abs. 2 BEKJ ist der Bundesrat nur zur Festlegung der Höhe der Gebühren befugt. Dass er in seinem Organisationsbereich noch mehr regeln darf, versteht sich von selber. Art. 18 liegt aber ausserhalb der Regelungskompetenz des Bunderats und verletzt die institutionelle Unabhängigkeit der Gerichte des Bundes (Art. 191c BV), zu der auch das Recht auf Selbstverwaltung gehört.

Art. 19: Die vorschussweise Bezahlung einer Gebühr ist eher aussergewöhnlich. Sachgerecht wäre es, wenn die Mitglieder der Körperschaft Mitgliederbeiträge zur Deckung der Grundkosten der Körperschaft bezahlen würden, die dann bei der Berechnung der Gebühren abgezogen würden. Art. 19 VEKJ zeigt auf, welche komplizierte, untaugliche Rechtsform die Trägerschaft aufweist.

Art. 20: Das ist eine perfektionistische Detailregelung, die in einer Verordnung des Bundesrats nichts zu suchen hat. Die Regelung ist auch unnötig, da man die Rechnung bei Fehlen einer „Rechnungsstelle“ einfach der Kantonsregierung zustellen könnte. Zudem wäre es sinnvoll, wenn auch allfällige Kantone, die nicht Mitglied sind, eine Rechnungsstelle bezeichnen würden.

Art. 21: Sachgerecht wäre, wenn die Evaluation nicht nur die Berechnung der Gebühr umfassen würde, sondern die Gesamtheit der Gebührenregelungen.

4.21 Artikel 22

4.21.1 Stellungnahme

4.21.1.1 Abs. 1

Vorschlag:

Der Absatz ist ersatzlos zu streichen.

Begründung:

Der Anwendungsbereich von Art. 22 Abs. 1 VEKJ kann nicht von jenem des Art. 29 Abs. 1 BEKJ abweichen.

4.21.1.2 Abs. 2

Vorschlag:

Der Absatz ist ersatzlos zu streichen.

Begründung:

Bei Art. 22 Abs. 2 entsteht ein innerer Widerspruch zu den Formatvorgaben in Art. 4 Abs. 3. Hier werden Scans formatmässig mit den „schriftlichen Unterlagen“ gleichgesetzt, was keinen Sinn ergibt. Dies ist ein weiterer Grund, weshalb Art. 4 Abs. 3 richtigerweise ersatzlos zu streichen ist.

Die Eingrenzung auf bestimmte Dateiformate wird als nicht sinnvoll erachtet, zumal gewisse PDF/A-Dateiformate wie beispielsweise PDF/A-3 als Formate für die Langzeitarchivierung nicht geeignet sind. Mit dem vorgeschlagenen Verweis auf die TR Resiscan oder gleichwertige Standards in Absatz 3 wird der Frage des Dateiformats des Scan-Outputs ausreichend Rechnung getragen.

4.21.1.3 Abs. 3 (neu, geändert)

Vorschlag:

3 Die Dokumente sind, soweit dies technisch möglich und für die jeweilige Vorlage geeignet ist, mittels Texterkennung durchsuchbar zu machen. Die Texterkennung dient der Auffindbarkeit und Weiterverarbeitung; sie ist nicht Teil der für die Übereinstimmung nach Absatz 4 massgebenden Bildebene.

Begründung:

Es erstaunt, dass der Verordnungsgeber sich beim ersetzenden Scannen auf Vorgaben wie mind. 300 DPI, 8-Bit Farbtiefe und OCR-Pflicht beschränkt, wo doch bspw. die TR Resiscan bekannterweise Wert auf organisatorische Massnahmen legt, die vor und nach dem Scanvorgang von Bedeutung sind und die das ersetzende Scannen auch aufwändig und teu(r)er machen. Die Anlehnung an den deutschen Standard RESISCAN ist sinnvoll, weil damit nicht nur technische Mindestwerte, sondern ein vollständiger Prozessansatz abgebildet wird: Vorbereitung, Scan, Vollständigkeitskontrolle, Umgang mit Sonderfällen, Protokollierung, Nachscan, Freigabe und Verantwortlichkeit.

Alleine schon die Anforderungen im TR Resiscan-Basismodul zeigen, dass es beim ersetzenden Scannen nicht nur um technische Vorgaben geht:

- Generelle Anforderungen (bspw. Verfahrensdokumentation), organisatorische Massnahmen (bspw. Abnahme- und Freigabe-Verfahren für Hardware und Software),
- personelle Massnahmen (bspw. Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung),
- technische Massnahmen (bspw. Generelle Sicherheitsmassnahmen für IT-Systeme im Scanprozess),
- Sicherheitsmassnahmen bei der Dokumentenvorbereitung (bspw. sorgfältige Vorbereitung der Papierdokumente und Vorbereitung der Vollständigkeitsprüfung),
- Sicherheitsmassnahmen beim Scannen (bspw. Protokollierung beim Scannen und Auswahl geeigneter Bildkompressionsverfahren),
- Sicherheitsmaßnahmen bei der Nachbearbeitung (bspw. geeignete und nachvollziehbare Nachbearbeitung) sowie
- Sicherheitsmassnahmen bei der Integritätssicherung (bspw. Nutzung geeigneter Dienste und Systeme für den Integritätsschutz).

Es wird deshalb vorgeschlagen, auf die BSI TR-03138 RESISCAN oder gleichwertige Standards zu verweisen. Entscheidend ist ein dokumentierter, risikobasierter End-to-End-Prozess. Wird ein Digitalisat nach einem solchen Verfahren erstellt und qualitätsgesichert, spricht eine Vermutung für die bildliche Richtigkeit und Vollständigkeit des Scans, solange keine konkreten gegenteiligen Anhaltspunkte bestehen, wie dies beispielweise bei Verwendung eines JBIG2-Filters der Fall sein könnte.

4.21.1.4 Abs. 4 (neu, geändert)

Vorschlag: *4 Der Bildlayer der Scan-Output-Datei muss vollständig, lesbar und dem physischen Dokument bildlich entsprechend sein. Die Qualitätssicherung umfasst insbesondere Vollständigkeit, Lesbarkeit, Seitenfolge, Farbwiedergabe, Auflösung, Behandlung von Sonderfällen und Dokumentation von Nachscans. Sie umfasst keine inhaltliche Prüfung der mittels digitaler Nachbearbeitung erzeugten weiteren Layer.*

Begründung:

Weder aus dem Verordnungstext noch aus dem erläuternden Bericht ergibt sich, was mit der «bildlichen» bzw. der «inhaltlichen» Übereinstimmung gemeint sein könnte. Weiter wird auch die Anforderung der «Übereinstimmung» nicht präzisiert. Der erläuternde Bericht hält fest, dass eine Überstimmung «visuell (Layout, Bilder)» wie auch «inhaltlich (Textgenauigkeit)» angestrebt werde. Diese Begrifflichkeit führt in die Irre. Texte in Scans sind als Bilddateien in einem Bildlayer angelegt, dasselbe gilt für weitere grafische Elemente wie Anordnung von Texten und von Abbildungen.

Zum geltend gemachten Ziel der «Übereinstimmung» ist festzuhalten, dass eine Datei als Ganzes betrachtet, die aus einem Scanvorgang entsteht, inhaltlich nie mit einem eingescannten Stück Papier übereinstimmen kann, weil ein Stück Papier und eine Datei offensichtlich nicht dasselbe sind. Jeder Scan-Output enthält Daten, die durch den Scanvorgang und einen allfällig folgenden OCR-Vorgang hinzugefügt wurde.[10] Es wird deshalb vorgeschlagen, den Scope der angestrebten Übereinstimmung technisch sauber einzugrenzen, und zwar auf den Bildlayer.

Die Qualitätskontrolle müsste sich dann nur auf den Bildlayer der Output-Datei und das Erscheinungsbild des Papier-Inputs beziehen. Sie würde insbesondere Vollständigkeit, Lesbarkeit, Seitenfolge, korrekte Zuordnung, Umgang mit Sonderformaten und Dokumentation von Nachscans umfassen. Der mittels OCR erzeugte Textlayer würde diesfalls nur der Auffindbarkeit und Weiterverarbeitung dienen (Such- und Hilfsebene). Er wäre nicht massgebend für die beweisrechtliche Übereinstimmung mit dem physischen Dokument und müsste nicht inhaltlich vollständig kontrolliert werden. Diese Eingrenzung erscheint notwendig, weil ein OCR-Layer zwar die Nutzbarkeit erhöht, aber bei Handschriften, Stempeln, Formularen, Tabellen, schlechten Vorlagen oder Mischdokumenten nie denselben Verlässlichkeitsgrad wie der Bildlayer aufweisen kann.

Die hier vorgeschlagene Vorgehensweise würde mit der Praxis in Österreich übereinstimmen, wo nur der Bildlayer Teil der Akte ist, der OCR-Layer aber nicht. Es wird dringend davon abgeraten, die Qualitätskontrolle auch auf den OCR-Layer auszudehnen, da eine solche Qualitätskontrolle erheblichen Aufwand für die ohnehin überlastete Justiz bzw. erhebliche Kosten für ein allenfalls ausgelagertes Scanning verursachen würde und Haftungsrisiken mit sich bringen würde. Selbstverständlich müsste diesem Umstand bei der Bearbeitung und Analyse von Verfahrensakten Rechnung getragen werden, indem Fundstellen aus dem OCR-Layer nötigenfalls mit dem Bildlayer abzugleichen wären, was mit der Justiz-Akten-Applikation JAA offenbar bereits heute technisch möglich ist.

4.21.1.5 Abs. 5 und 6 (neu)

Vorschlag:

5 Wurde ein Digitalisat in einem dokumentierten Verfahren erstellt, mit einem qualifizierten elektronischen Zeitstempel versehen und nach Absatz 4 qualitätsgesichert, wird vermutet, dass es dem physischen Dokument bildlich entspricht. Die Vermutung entfällt bei konkreten gegenteiligen Anhaltspunkten.

6 Das EJPD bezeichnet oder konkretisiert die Mindestanforderungen an Prozessdokumentation, Stichproben, Fehlerbehandlung, Nachscan, Protokollierung und Verantwortlichkeiten. Es berücksichtigt hierfür anerkannte Standards, namentlich die BSI TR-03138 RESISCAN oder gleichwertige Standards.

Begründung:

Vgl. Ausführungen zu Abs. 4 (neu)

4.21.1.6 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag: Die ersten zwei Sätze zu Art. 22 Abs. 3 sind zu streichen oder grundlegend zu Überarbeiten. (Von «Die Behörden müssen… bis verzerrte Abbildungen).

Begründung:

Die Begrifflichkeit in diesen zwei Sätzen sind aus digitalforensischer Perspektive falsch und führen zu Verwirrung. Beim Papierinput in einem Scanprozess muss es sich nicht zwingend um ein Original in Papierform handeln, auch Papierkopien können gescannt werden. Die vorgelagerten Schritte des

[10] Vgl. zur gleichen Thematik Marcel Steck / Claudia Schreiber, Beurkundungsrecht: Elektronische Verbale für die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen gemäss EÖBV, in: Jusletter 2. Juni 2025, Ziff. 2.2.5.9

Scanprozesses nach TR Resiscan dienen gerade dazu, festzustellen, ob das zu scannende Papierdokument ein Original oder eine Kopie darstellt.

Die Unterscheidung zwischen einer «visuellen Prüfung» und einer «inhaltlichen Prüfung» wie sie im zweiten Satz postuliert wird, macht weder technisch noch rechtlich einen Sinn und führt zu Verwirrung.

4.21.1.7 Neuer Art. 22a

Vorschlag:

Art. 22a Bereits bestehende digitale Aktenstücke und Dossiers

1 Digitale Aktenstücke und digitale Dossiers, die vor Inkrafttreten dieser Verordnung oder ausserhalb des Verfahrens nach Artikel 22 erstellt wurden, können als elektronische Aktenstücke beziehungsweise elektronische Dossiers im Sinne des BEKJ verwendet werden, wenn sie nach schriftlich dokumentierten Scanvorgaben erstellt, eindeutig zugeordnet, vollständig, lesbar und unverändert in die elektronische Akte übernommen werden können.

2 Die zuständige Behörde dokumentiert die Übernahme summarisch. Die Dokumentation enthält mindestens die Herkunft des Dossiers, den Zeitpunkt der Übernahme, das übernehmende System und allfällige festgestellte Einschränkungen.

3 Eine erneute Digitalisierung der Papierunterlagen ist nicht erforderlich, wenn die Voraussetzungen nach Absatz 1 erfüllt sind oder wenn keine Papierunterlagen mehr verfügbar sind und keine konkreten Zweifel an Vollständigkeit oder Lesbarkeit bestehen.

4 Bestehen konkrete Zweifel an Vollständigkeit, Lesbarkeit oder Zuordnung, ordnet die Behörde eine angemessene Nachprüfung, Ergänzung oder erneute Digitalisierung an.

Begründung:

Bereits heute werden trotz Papierprimat in vielen Verfahren elektronische Arbeitsdossiers erstellt. Wären diese nach Inkrafttreten des BEKJ generell nicht als digitale Dossiers verwendbar sein, entstünde ein erheblicher Aufwand.

Die Regelung sollte pragmatisch sein: Es wird keine rückwirkende Zertifizierung aller Altbestände angestrebt, aber eine nachvollziehbare Übernahme mit summarischer Dokumentation und Nachprüfung bei konkreten Zweifeln. «Schlecht» digitalisierte Verfahrensdossiers hingegen, die beispielsweise nicht nach bestimmten, schriftlich festgehaltenen Vorgaben gescannt wurden oder für deren korrekte Digitalisierung niemand die Verantwortung übernehmen will, müssten aber in jedem Fall erneut digitalisiert werden.

4.21.1.8 Neuer Art. 22b

Vorschlag:

Art. 22b Rücksendung physisch eingereichter Dokumente

1 Von der Rücksendung physisch eingereichter Dokumente nach Artikel 30 Absatz 1 BEKJ kann ohne anderslautendes vorgängiges Ersuchen der Absenderin oder des Absenders abgesehen werden, wenn:
a. das Dokument im Verfahren nicht nach Artikel 30 Absatz 2 BEKJ benötigt wird; und
b. dem physischen Exemplar kein eigenständiger Beweiswert zukommt oder ihm in digitalisierter Form derselbe Beweiswert zukommt.

2 Dies gilt namentlich für reine Mitteilungen, Ausdrucke elektronisch erstellter Dokumente, Fotokopien und Beilagen, deren Originale bei der Absenderin oder dem Absender verbleiben.

3 Vorbehalten bleibt die Rückbehaltung oder Rücksendung von Dokumenten, die forensisch relevante Spuren enthalten können, Urkundencharakter haben oder nach dem anwendbaren Prozess-recht im Original benötigt werden.

Begründung:

Namentlich im Strafverfahren gehen weiterhin grosse Mengen physischer Anzeigen, Beilagen und Mitteilungen ein. Eine pauschale Rücksendepflicht würde Porti, Versandarbeit und Verwaltungslast schaffen, ohne verfahrensrechtlichen Mehrwert zu bringen.

Zu unterscheiden ist zwischen blosser Mitteilung beziehungsweise Kopie und Papierstücken mit eigenständigem Beweiswert, etwa Originalurkunden in Papierform, handschriftlich unterzeichneten Dokumenten, Unterlagen mit Siegeln, Fingerabdrücken, DNA-Spuren oder sonstigen pertinenten forensischen Merkmalen.

4.21.1.9 Neuer Art. 22c

Vorschlag:

Art. 22c Zustellung von Papierkopien elektronisch erzeugter Dateien.

1 Führt eine Behörde ihre Akten elektronisch und erstellt sie ein Dokument, so versieht sie dieses mit dem gesetzlich vorgesehenen elektronischen Siegel, der erforderlichen elektronischen Signatur oder dem erforderlichen qualifizierten elektronischen Zeitstempel.

2 Muss ein solches Dokument Personen eröffnet werden, mit denen die Behörde nicht elektronisch verkehrt, kann die Eröffnung durch Zustellung eines Ausdrucks des elektronischen Dokuments erfolgen, sofern dieses ausgedruckt werden kann.

3 Die Zustellung der Papierkopie ist fristauslösend, wenn die angeschriebene Person auf dem Ausdruck darauf hingewiesen wird, dass sie das elektronische Dokumente kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein handschriftlich unterzeichnetes Exemplar verlangen kann.

Begründung:

Der Vorentwurf regelt den Trägerwandel vom Papier zur elektronischen Akte, nicht aber den praxisrelevanten umgekehrten Vorgang. Gerade bei Strafbefehlen, Verfügungen und anderen Massenprozessen wäre es systemwidrig, zusätzlich zum elektronischen Dokument regelmässig ein Papieroriginal mit eigenhändiger Unterschrift erstellen zu müssen.

Die Papierzustellung sollte als Notifikation beziehungsweise Ausdruck des elektronischen Dokuments verstanden werden. Andernfalls entstehen zwei nicht notwendigerweise kongruente Dokumente desselben Entscheids.

4.21.1.10 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag: Der Bericht ist zu korrigieren beziehungsweise zu ergänzen, damit keine neuen Papierpflichten entstehen. Er soll zwischen Papier-Originalen mit eigenständigem Beweiswert und einfachen Mitteilungen/Kopien in Papierform unterscheiden sowie Ausdrucke von Dateien zulassen, sofern ein Ausdrucken möglich ist und die Dateien jederzeit kostenlos nachverlangt werden können.

Mögliche Formulierung:

Art. 30 BEKJ ist so zu verstehen, dass physisch eingereichte Dokumente nicht unabhängig von ihrem verfahrensrechtlichen Gehalt zwingend zurückzusenden sind. Von einer Rücksendung kann insbesondere bei reinen Mitteilungen, Ausdrucken von Dateien und Fotokopien abgesehen werden, wenn die Absenderin oder der Absender keinen Rückversand verlangt und dem physischen Exemplar kein eigenständiger Beweiswert zukommt. Vorbehalten bleiben Dokumente mit Urkundencharakter oder möglichen forensischen Spuren.

Für elektronisch erzeugte Originaldokumente ist festzuhalten, dass deren Eröffnung an nicht elektronisch kommunizierende Personen mittels Ausdruck in Papierform möglich sein soll. Der Ausdruck ist keine zweite Originalfassung, sondern die teilweise physische Wiedergabe der Datei. Sie kann fristauslösend zugestellt werden, wenn auf die Möglichkeit hingewiesen wird, die Ausgangsdatei kostenlos zu beziehen oder einen handschriftlich unterzeichneten Ausdruck zu verlangen. Dem Ausdruck ist eine Erklärung beizugeben, wonach bestimmte Eigenschaften der Datei (bspw. Datei-Metadaten) im Ausdruck nicht enthalten sind.

4.22 Artikel 23

4.22.1 Stellungnahme

4.22.1.1 Einleitungssatz

Vorschlag: Technische Lösungen zur elektronischen Übermittlung von ~~Dokumenten~~ *Akten* nach Artikel 128b Absatz 2 der Zivilprozessordnung (ZPO), Artikel 103b Absatz 2 StPO und Artikel 8c Absatz 2 des

Opferhilfegesetzes vom 23. März 20072 (OHG) sind geeignet, wenn sie die folgenden Anforderungen erfüllen:

Begründung:

Es ist zwar durchaus richtig, dass es im Endeffekt um die Übermittlung von Dokumenten geht, die zitierten Gesetzesnormen regeln allerdings die „Weitergabe“ bzw. Übermittlung von „Akten“. Es wäre zielführend, auch in der VEKJ dieselbe Terminologie zu verwenden. Denn es geht bei Akten nicht um einzelne Dateien, sondern jeweils um eine Vielzahl von Dateien.

4.22.1.2 Bst. a

Vorschlag: ~~Der Zeitpunkt~~ *Die Zeitpunkte* der Übermittlung der ~~Akten~~ *in den Akten enthaltenen Dokumente* wird auf einer Quittung, in einem Protokoll oder auf andere Weise festgehalten~~; der Zeitpunkt der Übermittlung darf nur geändert werden, wenn dies auf der Quittung ausgewiesen wird.~~

Begründung:

Zum Begriff Zeitpunkte vgl. Ziffer 4.22.1.5 .Mit der vorgeschlagenen Formulierung wird eine Verbindung zwischen dem Begriff Akten und dem Begriff Dokumente (Dateien) hergestellt, die es dann ermöglicht, Bst. b und c im Sinne der übrigen Bestimmungen des VE-VEKJ zu formulieren. Der zweite Teilsatz von Bst. a ist falsch und zu streichen. Wenn gemäss Vorschlag zu Bst. b ein qualifizierter Zeitstempel verwendet werden muss, dann hält dieser den Zeitpunkt der Übermittlung fest und darf bzw. kann nicht geändert werden.

4.22.1.3 Bst. b

Vorschlag: Es wird ein ~~synchronisierter~~ qualifizierter Zeitstempel verwendet~~; die Abweichung zur offiziellen Zeit darf nicht mehr als eine Minute betragen.~~

Begründung:

Ein qualifizierter Zeitstempel hält die Zeitpunkte der Übermittlung fest. Der qualifizierte Zeitstempel weicht nicht von der offiziellen Zeit ab.

4.22.1.4 Bst. c

Vorschlag: Die Akte ist bei der Übermittlung ~~und in der Ablage~~ vor Veränderung und unberechtigter Kenntnisnahme geschützt. *In der Ablage sind Veränderungen von Dateien in einem Chain of Custody-Protokoll zu dokumentieren und die initialen Dateien sind verfügbar zu halten.*

Begründung:

Zahlreiche Ablagesysteme, die nicht auf die Speicherung von elektronischen Beweismitteln ausgerichtet sind, darunter auch die JAA, verändern Dateien. Beispielsweise indem aus dem entsprechenden Dossier Metadaten in Dateimetadatenfelder geschrieben werden oder indem Dateien in andere Dateiformate konvertiert werden (bspw. PDF zu einer Form von PDF/A). Es ist deshalb praxisfern, Veränderungen von Dateien verbieten zu wollen. Zielführender ist es, festzuhalten, dass die initial importierten Dateien unverändert verfügbar sein müssen und dass die vorgenommenen Änderungen jedenfalls bei elektronischen Beweismitteln in einem COC-Protokoll zu dokumentieren sind.

4.22.1.5 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag: In der Verordnung und im erläuternden Bericht soll einheitlich der Begriff «Zeitpunkte» der Übermittlung die Rede sein.

Begründung:

Im erläuternden Bericht ist zu Bst. a korrekterweise von den «Zeitpunkten der Übermittlung» (Plural) die Rede, während in Art. 23 Bst. a VE-VEKJ der Begriff «Zeitpunkt der Übermittlung» (Singular) verwendet wird. Wie sich aus Art. 5 Abs. 2 Bst. d-g ergibt, umfasst eine Übermittlung mehrere Etappen, die je zu einem individuellen Zeitpunkt erfolgen und je einzeln mit Quittung bestätigt werden. Zudem bestehen Akten aus mehreren Dateien, es können sich Situationen ergeben, in denen Bestandteile von Akten in

mehrere Etappen übermittelt werden (müssen). Auch aus diesem Grund drängt sich die Pluralformulierung auf.

Vorschlag: Der Text zu Bst. c ist entsprechend zu korrigieren.

Begründung:

Vgl. Begründung zu Bst. c.

4.23 Artikel 24

4.23.1 Stellungnahme

Vorschlag:

Art. 24 Abs. 1-5 (angepasst)

1 Abweichend von Artikel 128c Absatz 1 ZPO, Artikel 103c Absatz 1 StPO und Artikel 8d Absatz 1 OHG können die Behörden untereinander andere technisch geeignete Lösungen zur elektronischen Übermittlung von Dokumenten und verfahrensbezogenen Daten verwenden.

2 Bei der Übermittlung von Dokumenten müssen Zeitpunkte der Übermittlung, Absenderin oder Absender, Empfängerin oder Empfänger, Bezeichnung, Grösse und Hashwerte der Dokumente aufgezeichnet werden und unveränderbar sein.

3 Bei der Übermittlung strukturierter Daten müssen Zeitpunkte der Übermittlung, Absenderin oder Absender, Empfängerin oder Empfänger, Zweck beziehungsweise Verfahrensbezug, Art und Umfang der übermittelten Daten sowie eine geeignete Integritäts- und Nachvollziehbarkeitsinformation aufgezeichnet werden und unveränderbar sein. Anstelle von Hashwerten können namentlich Transaktionskennungen, Versionsstände, Ereignisprotokolle oder revisionssichere Audit-Trails verwendet werden.

4 Die Gewährung, Änderung oder Entziehung elektronischer Zugriffsrechte auf verfahrensbezogene Akten oder Daten gilt als elektronische Übermittlung, wenn Zeitpunkt, beteiligte Behörden, Umfang der Rechte und verantwortliche Benutzerinnen oder Benutzer beziehungsweise Benutzergruppen unveränderbar protokolliert werden.

5 Die Lösung muss den Schutz vor Veränderung und unberechtigter Kenntnisnahme gewährleisten. Sie darf nicht dazu dienen, die Plattformpflicht zu umgehen; zulässig sind insbesondere etablierte Fachschnittstellen, gemeinsame kantonale Systeme und technisch gleichwertige Behördenlösungen.

Begründung:

Der Austausch zwischen Staatsanwaltschaft und Polizei, der sich indirekt auf die Akteneinsicht durch Rechtsanwältinnen und Rechtsanwälte auswirkt, betrifft häufig strukturierte Daten, Statusmeldungen, Aufträge, Metadaten, Aktenstrukturen oder Zugriffsrechte und nicht nur PDF-Dateien. Eine rein dokumentenzentrierte Regelung provoziert Medienbrüche und künstliche Begleitdokumente.

Die Prinzipien der Chain of Custody, Datenschutz und Interoperabilität verlangen eine funktional gleichwertige Nachvollziehbarkeit, aber nicht zwingend dieselbe Logik wie dateibasierte Plattformübermittlungen. Bei Datenübermittlungen können Transaktions-IDs, Versionsstände, Schnittstellen-Logs und unveränderbare Audit-Trails sachgerechter sein als Hashwerte einzelner Dateien.

4.23.2 Weitere Bemerkungen zum erläuternden Bericht

Vorschlag:

Der Erläuternde Bericht muss klären, dass Art. 24 nicht nur dateibasierte Dokumentenübermittlungen, sondern auch verfahrensbezogene Datenübermittlungen und fachapplikationsbasierte Schnittstellen erfassen kann. Falls dies nicht gewollt ist, muss der Bericht ausdrücklich klarstellen, dass solche Übermittlungen ausserhalb des Geltungsbereichs des BEKJ liegen und anderweitig geregelt werden müssen.

Mögliche Formulierung:

Der Begriff der elektronischen Übermittlung unter Behörden umfasst neben der Übermittlung einzelner Dateien auch die Übermittlung strukturierter verfahrensbezogener Daten sowie die Gewährung oder Änderung von Zugriffsrechten in gemeinsamen oder gekoppelten Fachsystemen, sofern die Übermittlung funktional einer Weitergabe von Akten- oder Verfahrensinformationen entspricht.

Bei solchen Datenübermittlungen können die Anforderungen an Integrität und Nachvollziehbarkeit anders erfüllt werden als bei Dokumenten. Zulässig sind insbesondere revisionssichere Schnittstellenprotokolle, Transaktionskennungen, Versionsstände, Audit-Trails und Logfiles der beteiligten Fachsysteme. Hashwerte sind nur dort erforderlich, wo eine Datei oder ein eindeutig abgrenzbarer Datenexport übertragen wird. Die Regelung darf nicht zur Umgehung der Plattformpflicht dienen, sondern soll etablierte und sichere Behörden- und Fachschnittstellen ermöglichen.

4.24 Artikel 25

4.24.1 Stellungnahme

Diese Delegation der Rechtsetzungsbefugnis an das EJPD ist mit Art. 47 Abs. 1 RVOG nicht vereinbar. Das Festlegen der zulässigen Plattformen gemäss Art. 33b Abs. 2 SchKG ist keine rein technische Regelung von untergeordneter Bedeutung, sondern eine Regelung, die staatsrechtlich und allenfalls wirtschaftspolitisch bedeutsam ist.

4.25 Artikel 26

4.25.1 Stellungnahme

Vorschlag:

Art. 26 Abs. 1 bis 4 (ergänzend / präzisierend)

1 Protokolle und weitere Verfahrensakte können elektronisch bestätigt werden, wenn die bestätigende Person den zu bestätigenden Protokollinhalt in geeigneter Weise zur Kenntnis nehmen kann und die Bestätigung unveränderbar mit dem Protokoll verbunden wird.

2 Die elektronische Bestätigung kann mittels handschriftähnlicher elektronischer Unterschrift auf einem Signaturgerät erfolgen. Sie umfasst mindestens die bildliche Wiedergabe der Unterschrift, den Zeitpunkt der Bestätigung, die eindeutige Zuordnung zum Protokoll und einen Integritätsschutz des bestätigten Dokuments.

3 Werden biometrische Signaturdaten erhoben, so sind die Mindestanforderungen an zeitliche Auflösung, räumliche Auflösung, Druckerfassung, Bewegungsdaten, Speicherung, Verschlüsselung, Protokollbindung, Prüfbarkeit und Löschung auf geeigneter Stufe zu bezeichnen. Dabei sind anerkannte Standards, namentlich ISO/IEC 19794-11 oder gleichwertige Nachfolgestandards, zu berücksichtigen.

4 Die audiovisuelle Aufzeichnung einer Verfahrenshandlung entbindet nicht von der Erstellung und Bestätigung des gesetzlich vorgeschriebenen Verfahrens- beziehungsweise Rahmenprotokolls.

Begründung:

Namentlich in Strafverfahren bleibt die Unterzeichnung von Protokollen zentral. Auch bei audiovisueller Aufzeichnung dokumentiert das Verfahrens- beziehungsweise Rahmenprotokoll zusammen mit der Aufzeichnung die Verfahrenshandlung und muss von den Beteiligten bestätigt werden. Die blosse Aufzählung von Datenkanälen wie Strichbeschaffenheit, Druck, Bewegungsfluss, Bewegungsrichtung und Zeitpunkt genügt nicht. Entscheidend sind Mindestqualität, Prüfbarkeit, Integritätsschutz, Bindung an das konkrete Protokoll und Interoperabilität zwischen Fachapplikationen und Signaturdiensten. Beschaffungs- und Implementierungsrisiken lassen sich vermeiden, wenn die Verordnung beziehungsweise die technische Konkretisierung Mindestanforderungen festlegt und die Orientierung an ISO/IEC 19794-11 ausdrücklich zulässt, ohne damit alle fachlichen Qualitätsfragen als erledigt zu betrachten.

4.26 Kapitel X (neu). Eindeutige Identifikation von Aktenstücken

Vorschlag:

Kapitel X. Eindeutige Identifikation von Aktenstücken (neu)

Art. XX Eindeutige Identifikation der Aktenstücke (neu)

1 Jedes elektronische Aktenstück ist bei seiner Erstellung, Entgegennahme, Digitalisierung, Übernahme oder Migration in ein elektronisches Dossier mit einem eindeutigen, dauerhaft unveränderlichen technischen Identifikator zu versehen. Bei entgegengenommene Aktenstücken ist das initial übermittelte Aktenstück unverändert ebenfalls zu speichern.

2 Der Identifikator ist als UUID auszugestalten.

3 Der Identifikator ist als Metadatum des Aktenstücks zu führen. Er ist bei Export, Übermittlung, Migration, Archivierung und Wiederverwendung des Aktenstücks mitzuführen.

4 Der Identifikator ersetzt weder Geschäftsnummern, Aktenzeichen, Dokumenttitel, Aktenverzeichniseinträge noch andere fachliche oder verfahrensrechtliche Bezeichnungen.

5 Für bereits bestehende elektronische Dossiers, insbesondere Legacy-Scans und andere vor Inkrafttreten des BEKJ erstellte digitale Dossiers, ist der Identifikator spätestens bei deren Übernahme in ein elektronisches Dossier nach BEKJ zu erzeugen. Die Zuordnung ist nachvollziehbar zu protokollieren.

6 Das Fehlen oder die nachträgliche technische Korrektur eines Identifikators berührt die verfahrensrechtliche Gültigkeit eines Aktenstücks nicht, sofern dessen Herkunft, Inhalt und Zuordnung auf andere Weise zuverlässig nachvollziehbar sind.

Begründung:

Die eindeutige technische Identifikation jedes Aktenstücks ist eine zentrale Voraussetzung für eine verlässliche elektronische Aktenführung. Ein UUID erlaubt es, ein Aktenstück über seinen gesamten Lebenszyklus hinweg systemübergreifend eindeutig zu referenzieren, unabhängig davon, ob sich Dateinamen, Dokumenttitel, Aktenverzeichniseinträge, Speicherorte oder technische Ablagestrukturen ändern.

Die Vorgabe dient insbesondere der Nachvollziehbarkeit bei Scanprozessen, bei der Übermittlung zwischen Behörden, bei der Migration bestehender elektronischer Dossiers, bei der Zwischen- und Langzeit-Archivierung sowie bei der späteren Wiederverwendung oder erneuten Bereitstellung von Aktenstücken. Sie reduziert das Risiko von Verwechslungen, Dubletten, Medienbrüchen und fehlerhaften Zuordnungen.

Der UUID ist nicht als neue verfahrensrechtliche Aktennummer zu verstehen. Er hat rein technische Identifikationsfunktion und ersetzt weder Geschäftsnummern noch Aktenzeichen oder fachliche Dokumentbezeichnungen. Ebenso soll die Bestimmung keine zusätzliche formelle Gültigkeitsvoraussetzung für Aktenstücke schaffen. Fehler bei der Vergabe oder Führung des Identifikators sind technisch und organisatorisch zu korrigieren, sollen aber nicht ohne Weiteres die rechtliche Verwertbarkeit eines Aktenstücks in Frage stellen.

Besonders wichtig ist die Regelung für bestehende digitale Dossiers und Legacy-Scans. Bereits heute werden in der Praxis trotz Papierprimat elektronische Arbeitsdossiers geführt. Diese müssen nach Inkrafttreten des BEKJ ohne unnötige Neudigitalisierung oder manuelle Neuerfassung als vollwertige digitale Dossiers weiterverwendet werden können. Die nachträgliche Vergabe eines UUID schafft hierfür eine einfache, robuste und nachvollziehbare technische Brücke.

4.27 Stellungnahme zum Anhang 1 VE-VEKJ

Die vollständige Aufhebung der VeÜ-VwV ist voreilig. Bei dieser Verordnung geht es teilweise um grundlegend andere Fragen, die das VEKJ gar nicht adressiert, z.B. die Modalitäten der elektronischen Verfügungseröffnung oder bestehende elektronischen Kommunikationskanäle der Bundesbehörden. Es ist sorgfältig zu prüfen, welche Normen der VeÜ-VwV es nach wie vor braucht, bis die VwVG-Plattform tatsächlich betriebsbereit ist und alle derzeit in der VeÜ-VwV geregelten Fragen anderweitig geregelt sind.

5 Anhang

5.1 Leitsätze

5.1.1 Generelle Leitsätze

5.1.1.1 A. Zugang zum Recht

Leitsatz #A1

Justitia 4.0 soll den Zugang zum Recht erleichtern.[11]

Leitsatz #A2

Justitia 4.0 soll den Zugang zum Recht für alle, auch die professionellen Akteure erleichtern, nicht erschweren oder sonst wie einschränken.[12]

5.1.1.2 B. Verhältnis zur gesetzlichen Grundlage

Leitsatz #B1

Ein formelles Bundesgesetz muss festhalten, welche Daten im Zusammenhang mit der Plattform Justitia.swiss und den mit ihr verbundenen kantonalen Plattformen gesammelt werden dürfen, von wem sie bearbeitet werden dürfen und welche Bearbeitungen nicht erlaubt sind.[13]

Leitsatz #B2

Die Datenhaltung und Datenspeicherung über den elektronischen Rechtsverkehr ist auf ein absolut technisch erforderliches Minimum zu beschränken.[14]

5.1.1.3 C. Zum sachlichen Fokus

Leitsatz #C1

Die Kernanliegen an Justitia 4.0 sind aus der Perspektive der Rechtsanwälte

a) elektronische Unterlagen senden,

b) elektronische Unterlagen erhalten und

c) Akteneinsicht sicherstellen.[15]

Leitsatz #C2

---

[11] In der Schweiz ist der Zugang zum Recht seit jeher bürgerfreundlich ausgestaltet. Von vergleichsweise laienfreundlichen Gesetzestexten bis hin zu einer Vielzahl von prozessualen Erleichterungen für nicht anwaltlich vertretene Rechtsuchende kennt die Justiz grosse Entgegenkommen im Zugang zum Recht. Die Digitalisierung ist hier gleichzeitig Chance und Gefahr. Die Anwaltschaft erwartet, dass Justitia 4.0 in dieser Hinsicht Chancen nutzt und den Zugang zum Recht weiter erleichtert. Dies sowohl für nicht anwaltlich vertretene, als auch für anwaltlich beratene Rechtssuchende. Der Zugang zum Recht soll durch die geplante Justizplattform somit nicht primär "technisiert", sondern weiter pragmatisch geöffnet werden. Gleichzeitig ist vor der Gefahr zu warnen, dass elektronische Eingaben an Justizbehörden zum Beispiel durch den heute zum Standard gewordenen legeren Umgang mit elektronischer Korrespondenz "trivialisiert" werden. Rechtssuchende – auch Laien – müssen wissen, dass sie mit einer Eingabe an eine Justizbehörde rechtswirksame Handlungen u.U. mit grossen Kostenfolgen vornehmen.

[12] Die Anwaltschaft ist im Zuge der Digitalisierung bereits mit einer Vielzahl von Herausforderungen konfrontiert. Der Klientenverkehr wird schnelllebiger. Die Kommunikation mit Korrespondenzpartnern kann aufgrund vieler verschiedener Systeme oft nicht medienbruchfrei sichergestellt werden. Die Anwaltschaft will sich diesen Herausforderungen stellen. Sie erwartet indes, hierbei von den Justiz- und Verwaltungsbehörden, welche teilweise den gleichen Erwartungen ausgesetzt sind, unterstützt zu werden. Die Justizplattform der Zukunft darf daher die Anwaltschaft in ihren Prozessen nicht einschränken. Die Plattform ist in ihren Rollenvorgaben so zu gestalten, dass die Anwaltschaft frei bleibt. Diese Tätigkeit ist von der Wirtschaftsfreiheit geschützt und Vorbedingung, dass dem Grundsatz des Zugangs zum Recht zum Durchbruch verholfen wird.

[13] Nach den geltenden Grundsätzen zum Datenschutz müssen sämtliche grösseren Datenbank-Anwendungen und Plattformen über eine formell-gesetzliche Grundlagen verfügen. Zum Beispiel gesetzliche Grundlagen für Informationssysteme im Bereich Sport.

[14] Die elektronische Plattform soll die bisherige analoge, schriftliche Behördenkommunikation ergänzen oder ersetzen, und nicht zusätzliche Datengrundlagen für Auswertungen und Analysen mit unabsehbaren Folgen für alle Beteiligten schaffen.

[15] In diesen drei vorgenannten Bereichen liegt der grösste Nutzen einer Digitalisierung, so kann analoge, schriftliche Korrespondenz reduziert werden.

Die Funktionalität der zentralen Plattform von Justitia 4.0 (Justitia.swiss) soll sich an den Kernanliegen orientieren.

5.1.1.4 D. Code is Law

Leitsatz #D1

Justitia 4.0 darf keine technischen Pfadabhängigkeiten schaffen.[16]

Leitsatz #D2

Justitia 4.0 darf Recht nicht verunmöglichen, insbesondere darf Justitia 4.0 nicht das Verfassungs- und Verfahrensrecht aushöhlen.

Leitsatz #D3

Die Plattform Justitia.swiss wird nach dem Prinzip der Konfigurierbarkeit aufgebaut.[17]

Leitsatz #D4

Das Projekt Justitia 4.0 muss offenlegen, welche der Spezifikationen für den Bau und den Betrieb der Plattform Gesetzesänderungen verlangen.

Leitsatz #D5

Die Plattform Justitia 4.0 muss interoperabel und betriebssystemunabhängig sein (andere vertrauliche elektronische Kommunikation) und die direkte Integration in verschiedene Fachanwendungen zulassen.[18]

Leitsatz #D6

Die Plattform muss über eine Notfallplanung verfügen. Im Notfall muss eine funktionierende alternative Form der elektronischen Übermittlung jederzeit zur Verfügung stehen.

Leitsatz #D7

Der Anwalt darf in keinem Fall (unabhängig vom Beweismass) die Beweislast dafür tragen müssen, dass die Plattform funktionsfähig oder nicht funktionsfähig war.[19]

5.1.2 Leitsätze zu den Akteuren im Justizwesen, die öffentliche Aufgaben wahrnehmen

5.1.2.1 E. Neue Rollen der Akteure im Justizwesen

Leitsatz #E1

[16] Als sogenannte Pfadabhängigkeiten wird hier eine technische bzw. durch die Plattform Justitia 4.0 unabänderlich oder nur schwer abänderliche Vorkehrung, die Arbeitsabläufe oder sonstige Abläufe (z.B. auf Seiten der Anwaltschaft) erzwingt, die bislang – ohne solche Pfadabhängigkeiten – im Belieben der Berufsträgerin oder des Berufsträgers gestanden hätten. Pfadabhängigkeiten führen stets zu einer Standardisierung und einer Einschränkung der Individualisierung.

[17] Konfigurierbarkeit ist hier zu verstehen als Methode der Programmierung, bei der grundsätzlich und wo immer möglich individuell anpassbare Parameter einer „harten Programmierung“ vorgezogen werden.

[18] Die Anwaltschaft arbeitet heute mit einer Vielzahl verschiedener Fachapplikationen und Betriebssystemen. Um faire Marktbedingungen zu gewährleisten, müssen diese Systeme mit der Plattform kommunizieren können.

[19] Da der/die Anwalt/Anwältin keinerlei Kontrolle über die elektronische Plattform hat und auch keinen Zugriff auf deren IT-Daten besitzt, ist er/sie nicht in der Lage, eine allfällige Fehlfunktion nachzuweisen. Wenn sich ein(e) Anwalt/Anwältin über eine Störung beklagt, hat die für den Betrieb der Plattform zuständige Stelle den Nachweis des ordnungsgemässen Funktionierens zu erbringen oder die Fehlfunktion zu bestätigen. Es erscheint sinnvoll, ein einfaches und rasches Verfahren einzuführen, um im Falle einer Störung Zweifel wirksam auszuräumen, was das Vertrauen in das neue elektronische Kommunikationssystem stärken würde /// L'avocat(e) n'ayant aucune maîtrise sur la plateforme électronique ni accès aux données informatiques de cette dernière, il/elle n'est pas à même de prouver un éventuel dysfonctionnement. Si un(e) avocat(e) se plaint d'un dysfonctionnement, l'entité qui gère la plateforme devra apporter la preuve du bon fonctionnement ou confirmer le dysfonctionnement. Il semble judicieux de mettre en place une procédure simple et rapide pour lever efficacement les doutes en cas de dysfonctionnement, ce qui renforcerait la confiance dans le nouveau système de communication électronique.

Niemand soll im Zusammenhang mit Justitia 4.0 eine Überwachungsfunktion über die Kommunikation zwischen den Akteuren des Justizwesens übernehmen bzw. erhalten.[20]

Leitsatz #E2

Die Akteure im Justizwesen, die öffentliche Aufgaben wahrnehmen, sollen im Zusammenhang mit Justitia 4.0 keine Administrationsfunktion über andere Akteure des Justizwesens einnehmen und keine Administrationsaufgaben erhalten.[21]

Leitsatz #E3

Akteure, die öffentliche Aufgaben wahrnehmen, sollen keine neuen Aufgaben übernehmen, es sei denn, dies entspreche einer sachlichen Notwendigkeit, die mindestens von einem weiteren Leitsatz getragen werden und für die eine formelle gesetzliche Grundlage bestehen müsste.[22]

5.1.3 Leitsätze zu den Pflichten und Rechten von Rechtsanwälten

5.1.3.1 F. Neue Rollen oder neue Pflichten für die Anwaltschaft

Leitsatz #F1

Rechtsanwältinnen und Rechtsanwälte sollen weiterhin die Möglichkeit haben, fristwahrend analoge Eingaben an die Behörden zu übermitteln (bedingungsloses, auch fallweises Opt-Out).[23]

Leitsatz #F2

Rechtsanwältinnen und Rechtsanwälte sollen ohne entsprechende (Vergütung) Entschädigung keine von den Behörden im Rahmen von Justitia 4.0 an sie ausgelagerte Aufgaben übernehmen müssen.[24]

Leitsatz #F3

Rechtsanwältinnen und Rechtsanwälte, die nicht-anwaltlicher Funktion als Teilnehmer auf der Plattform mitwirken, sollen dies unter einer oder mehreren von der beruflichen Identität als Rechtsanwalt unterschiedenen privaten oder anderweitig beruflichen Identität(en) tun können. Die verschiedenen Identitäten dürfen nicht miteinander in Verbindung gebracht werden können.[25]

Leitsatz #F4

Fristenwahrung, Zustellung: Ein formelles Gesetz muss die Fristenwahrung regeln. Die elektronische Zustellung muss seine Regelung analog der heutigen Regelung mit eingeschriebener Post (Abholfrist von 7 Tagen) vorsehen. Dem Anwalt müssen unmittelbar beweiskräftige Quittungen ausgestellt werden, mit denen er die Fristwahrung beweisen kann.[26]

---

[20] Eine Anwaltsaufsicht darf beispielsweise nicht in die via Plattform gemäss BEKJ oder via mit dieser Plattform verbundene kantonale Datensammlungen Kommunikationsdaten eines RA Einsicht nehmen, um festzustellen, ob dieser öfters Fristen verpasst oder zugestellte Unterlagen erst in letzter Minute abholt.

[21] Zu solchen Administrationsaufgaben könnte gehören: Feststellung der Eintragung im kantonalen Anwaltsregister.

[22] Zu solchen neue Aufgaben könnten gehören: Den Anwaltswechsel auf Wunsch eines Klienten organisatorisch auf der Plattform durchführen (Rechte entziehen, Rechte neu vergeben).

[23] Eine zweckmässige und funktionierende elektronische Plattform würde bei der Anwaltschaft von selbst genügend Attraktivität für eine Übernahme generieren. Die Digitalisierung durch einen gesetzlichen Zwang erzwingen zu wollen, halten wir jedoch für verfehlt und gefährlich, und für einen unzulässigen Eingriff in die Berufs- und Wirtschaftsfreiheit der Anwälte.

[24] Zu solchen ausgelagerten Aufgaben gehören u.a. das Scannen und Ausdrucken von Verfahrensakten und das Erfassen von Fall/Dossier-Metadaten. Eine Verkoppelung von Anforderungen und Entschädigung ist nötig.

[25] Der vorliegende Leitsatz stellt das Postulat auf, dass es für RA mindestens drei Identitäten braucht: a) beruflich als RA BGFA, b) beruflich als nicht-RA, c) privat als Staatsbürger.

[26] Der Zeitpunkt der Zustellung sowie der für die Wahrung einer Frist massgebende Zeitpunkt sind in den Verfahrensordnungen (formelle Gesetze) klar geregelt. Gleiches muss für die elektronische Kommunikation gelten. Es besteht kein Anlass, von der allgemeinen Regel abzuweichen, wonach eine Frist gewahrt ist, wenn die Eingabe am letzten Tag der Frist abgesandt oder eingereicht wird. Massgebend muss daher der Zeitpunkt der Absendung durch die Anwältin oder den Anwalt sein und nicht der Zeitpunkt, zu dem die Plattform beziehungsweise der Empfänger die Dokumente erhält. Analog zu eingeschriebenen Briefen muss der Anwalt zudem unverzüglich eine elektronische Bestätigung über die Absendung sowie anschliessend eine Bestätigung über die Zustellung an den Empfänger erhalten. Ebenso besteht kein Grund, bei der elektronischen Kommunikation auf das siebentägige Abholfrist-System zu verzichten. Diese Frist ist notwendig, um dem Anwalt zu ermöglichen, während einer

Woche von der Kanzlei abwesend zu sein, ohne dass – teils sehr kurze – Rechtsmittelfristen während seiner Abwesenheit zu laufen beginnen.

Bundesanwaltschaft
Ministère public de la Confédération
Ministero pubblico della Confederazione
Procura publica federala

CH-3003 Berne, MPC

Par courriel à cornelia.perler@bj.admin.ch
Département fédéral de justice et police
Office fédéral de la justice
Mme Cornelia Perler
Bundesrain 20
3003 Berne

Juriste Service juridique: Almedina Zrinic
Juriste Service juridique: Besna Karatas
Numéro de procédure: RD.25.0089-ZRA
Berne, 3 juin 2026

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP) – ouverture de la procédure de consultation

Madame,

Nous revenons à la procédure de consultation citée en marge et vous remercions de nous avoir donné la possibilité de prendre position. Vous trouverez ci-dessous la prise de position du Ministère public de la Confédération (« MPC »).

Concernant le projet d'ordonnance :

- De manière générale, une discrépance entre la version allemande et les versions française et italienne de l'ordonnance subsiste concernant la mention du MPC. En effet, en allemand le nom complet de l'autorité (« *Bundesanwaltschaft* ») est utilisé alors que seule l'abréviation (« MPC ») l'est en français et en italien. Pour des raisons systématique et stylistique, il convient d'utiliser le nom complet de l'autorité au niveau de l'ordonnance dans les trois langues.

- Art. 17 al. 2 OCEP : Cet article prévoit que le Conseil fédéral décide tous les trois ans de la répartition de la part de l'administration fédérale et du MPC entre les départements, la Chancellerie fédérale et le MPC. Or, le MPC ne sera ni membre de l'Assemblée au sens de l'art. 9 LPCJ ni du comité au sens de l'art. 10 LPCJ de la

Ministère public de la Confédération MPC
Almedina Zrinic
Guisanplatz 1
3003 Berne
Tél. +41 58 480 88 05
www.bundesanwaltschaft.ch

corporation de droit public à créer, bien qu'il soit actuellement membre du projet Justitia 4.0. Le MPC n'aura donc pas de droit de participation concernant les décisions relatives aux émoluments alors qu'il sera contributeur. Par ailleurs, le MPC étant une autorité autonome indépendante qui ne fait plus partie de l'administration fédérale.

Wichtig erscheint uns in Bezug auf die Vertretung der BA in der Versammlung bzw. dem Vorstand sowie der Festlegung der Gebühren der zentralen Plattform der Blick auf die Entstehungsgeschichte des BEKJ: Während auf Stufe Bund für die Bundesverwaltung (vertreten durch das EJPD) und das Bundesgericht stets eine Vertretung in der Trägerschaft der zentralen Plattform vorgesehen war (siehe Art. 9 und 10 VE BEKJ), sah der Gesetzesentwurf nicht vor, dass die BA in diesen beiden Gremien vertreten sein sollte. Die BA ersuchte bereits im Rahmen ihrer Stellungnahme zur ÄK vom 10. Juli 2020, dass im Falle einer finanziellen Beteiligung der BA diese auch in der Versammlung und im Vorstand vertreten sein sollte.

Mit dem vollständigen Inkrafttreten des BEKJ wird die BA zur elektronischen Übermittlung von Dokumenten (Art. 103c und 103d E-BEKJ) verpflichtet und für die Nutzung der zentralen Plattform werden Gebühren anfallen. Als Gegengewicht dazu steht u.E. auch der BA – wie dem EJPD, den Vertretern der Kantone sowie dem Präsidenten des Bundesgerichts (siehe Art. 9 Abs. 2 und Art. 10 Abs. 2 E-BEKJ) eingeräumt – eine entsprechende Teilnahme in der Versammlung und dem Vorstand zu. Dass dies im Rahmen des BEKJ nicht erfolgte, erachten wir als gesetzgeberisches Versehen und ersuchen Sie als federführendes Amt, dem Parlament im Rahmen einer nächsten parlamentarischen Beratung den Antrag zu unterbreiten, dass sowohl Art. 9 Abs. 2 (für die Versammlung) und Art. 10 Abs. 2 E-BEKJ (für den Vorstand) mit Bst. d «dem Bundesanwalt oder einem seiner Stellvertreter» zu ergänzen sei. Zudem sei Art. 16 Abs. 1 E-VEKJ so anzupassen, dass die Bundesanwaltschaft mit einer (verhältnismässigen) prozentualen Beteiligung unter Bst. d separat aufgeführt und ebenso der «Gebührenanteil der Bundesanwaltschaft» mit einem neuen Artikel (z.B. Art. 18a E-VEKJ) erfasst wird.

Compte tenu de ce qui précède, il semble opportun de prévoir, à tout le moins dans l'ordonnance, un droit de consultation du MPC lors de la fixation de sa part des 5% dévolus à ce dernier et à l'administration fédérale. Nous proposons de prévoir que la répartition entre l'administration fédérale et le MPC est convenue entre le Conseil fédéral et le MPC. Aussi, nous proposons la modification suivante de l'art. 17 al. 2 OCEP :

« [2] Der Bundesrat und die Bundesanwaltschaft vereinbaren den Anteil der Bundesverwaltung und denjenigen der Bundesanwaltschaft. Der Bundesrat legt die Aufteilung des Anteils der Bundesverwaltung ~~und der Bundesanwaltschaft~~ auf die Departemente und die Bundeskanzlei ~~und die Bundesanwaltschaft~~ jeweils für drei Jahre fest.»
« [2] Le Conseil fédéral et le Ministère public de la Confédération conviennent de la part de l'administration fédéral et de celle du Ministère public de la Confédération. Le Conseil fédéral décide tous les trois ans de la répartition de la part de l'administration fédérale ~~et du Ministère public de la Confédération~~ entre les départements et la Chancellerie fédérale ~~et le Ministère public de la Confédération~~. »

Au vu de ce qui précède, il convient également de tenir compte de ce changement et d'adapter le rapport explicatif relatif à l'art. 17 al. 2 OCEP en conséquence (voir proposition ci-dessous).

Concernant rapport explicatif :

- Art. 4 al. 4 et 5 OCEP : une discrépance entre la version allemande et français subsiste dans la formulation relative aux formats que les tribunaux et d'autres autorités *peuvent lire* (formulation francophone). La version en langue allemande prévoit, en revanche, qu'il s'agit des formats *utilisés* par ces mêmes autorités ce qui pourrait laisser entendre qu'elles peuvent décider sous quels formats les preuves doivent par exemple être transmises. Le MPC privilégie la formulation en langue française, soit uniquement la possibilité pour les tribunaux et les autres autorités d'indiquer les formats qu'elles peuvent lire sans toutefois pouvoir imposer de format limitatif par rapport à l'art. 4 al. 3 OCEP. Il convient donc d'adapter la version en langue allemande.

- Art. 16 OCEP : la formulation actuelle dans le rapport explicatif prête à confusion et semble inclure le MPC dans l'administration fédérale (ad art. 16 al. 1 let. a OCEP, p. 28 : « *La part de la Confédération sera financée à parts égales par l'administration fédérale et par les tribunaux de la Confédération.* […] »). Aussi, nous proposons de préciser qu'il s'agit du financement pour l'administration fédérale et le MPC (également dans la version en allemand). Nous proposons donc d'ajouter la mention du MPC dans le rapport explicatif :

  «Der Anteil des Bundes wird je zur Hälfte von der Bundesverwaltung und der Bundesanwaltschaft sowie von den eidgenössischen Gerichten getragen. […]»
  « *La part de la Confédération sera financée à parts égales par l'administration fédérale et le MPC ainsi que par les tribunaux de la Confédération.* […] »).

- Art. 17 al. 1 OCEP : la formulation actuelle dans le rapport explicatif prête à confusion et semble inclure le MPC dans l'administration fédérale (ad art. 17 al. 1, p. 28 : « *Le DFJP versera l'émolument dû par l'administration fédérale* »). Cette formulation ne correspond d'ailleurs pas au texte de l'ordonnance qui stipule que le DFJP verse l'émolument qui doit être financé par l'administration fédérale et par le MPC. Aussi, nous proposons d'ajouter la mention du MPC dans le rapport explicatif :

  « Das EJPD bezahlt die von der Bundesverwaltung und der Bundesanwaltschaft geschuldete Gebühr. […]»
  « Le DFJP versera l'émolument dû par l'administration fédérale et par le MPC. […] »

- Art. 17 al. 2 OCEP : La formulation actuelle dans le rapport explicatif prête à confusion et semble inclure le MPC dans l'administration fédérale (ad art. 17 al. 2, p. 28 : « *Le Conseil fédéral décide de la répartition de la part de l'administration fédérale au sein de celle-ci, à savoir entre les départements, la Chancellerie fédérale et le MPC, et ce pour trois ans.* »). Par ailleurs, il convient de tenir compte de notre proposition de modification de l'art. 17 al. 2 OCEP (ci-dessus). Aussi, nous proposons la modification suivante du rapport explicatif relatif à l'art. 17 al. 2 :

  « Da die Bundesanwaltschaft eine unabhängige und selbständige Behörde ist, vereinbaren der Bundesrat und die Bundesanwaltschaft gemeinsam die jeweiligen

Anteile der Bundesverwaltung und der Bundesanwaltschaft. Diese Lösung trägt dem Umstand Rechnung, dass die Bundesanwaltschaft weder Mitglied der Versammlung im Sinne von Art. 9 BEKJ noch des Vorstands im Sinne von Art. 10 BEKJ der zur gründenden Körperschaft des öffentlichen Rechts sein wird. Der Bundesrat legt die interne Aufteilung des Bundesverwaltungsanteils auf die Departemente und die Bundeskanzlei ~~und die Bundesanwaltschaft~~ jeweils für drei Jahre fest. Damit erfolgt ein einheitlicher und politisch legitimierter Umlageentscheid ~~für die Bundesverwaltung~~. Aufgrund der dreijährigen ~~mehrjährigen~~ Gebührenfestsetzung ergibt sich auch Sicherheit in der Planung.»
« Le MPC étant une autorité autonome indépendante, le Conseil fédéral et le MPC conviennent ensemble de la part de l'administration fédérale et de celle du MPC. Cette solution tient compte du fait que le MPC ne sera ni membre de l'Assemblée au sens de l'art. 9 LPCJ ni du comité au sens de l'art. 10 LPCJ de la corporation de droit public à créer. Le Conseil fédéral décide de la répartition de la part de l'administration fédérale au sein de celle-ci, à savoir entre les départements et la Chancellerie fédérale ~~et le MPC~~, et ce pour trois ans. La répartition des frais fait ainsi l'objet d'une décision uniforme jouissant d'une légitimité politique. Le fait que la répartition soit fixée tous les trois ans contribue également à la sécurité de la planification. »

- Art. 18 al. 1 OCEP : la formulation actuelle dans le rapport explicatif prête à confusion et semble inclure le MPC dans l'administration fédérale (ad art. 18 al. 1 OCEP : « […]. *Il joue le même rôle que le DFJP pour l'administration fédérale et centralise le paiement de la part relevant de l'ensemble de la juridiction fédérale.* […] »). Aussi, nous proposons de préciser qu'il s'agit du rôle pour l'administration fédérale et le MPC (également dans la version en allemand). Aussi, nous proposons la modification suivante du rapport explicatif relatif à l'art. 18 al. 1 :

  « […] Dadurch zentralisiert das Bundesgericht, gleich wie bei der Bundesverwaltung und der Bundesanwaltschaft, die 30/40 Zahlung nach aussen für die gesamte Gerichtsbarkeit des Bundes. […] »
  « […]. *Il joue le même rôle que le DFJP pour l'administration fédérale et le MPC et centralise le paiement de la part relevant de l'ensemble de la juridiction fédérale.* […] »).

Les modifications proposées devront également être reprises en italien.

Nous restons à votre disposition pour tout complément. Les questions complémentaires peuvent être adressées directement à l'adresse aemterkonsultationen@ba.admin.ch.

Nous vous prions, Madame, de bien vouloir examiner nos demandes et de l'assurance de notre considération distinguée.

Ministère public de la Confédération MPC



Stefan Blättler
Procureur général de la Confédération

Bundesgericht

Tribunal fédéral

Tribunale federale

Tribunal federal

Der Generalsekretär
Av. du Tribunal fédéral 29
CH - 1000 Lausanne 14
Tel. +41 (0)21 318 91 11
www.bger.ch
Geschäftsnummer 003.1
DOCID 15366002

Eidg. Justiz- und Polizeidepartement
Bundesamt für Justiz
Herr Bundesrat
Beat Jans
3003 Bern

Versand per E-Mail
cornelia.perler@bj.admin.ch

Lausanne, 22. Mai 2026 / BrJ

Stellungnahme bezüglich Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat

Wir danken Ihnen für die Möglichkeit zur Stellungnahme anlässlich der Vernehmlassung zum oben erwähnten Verordnungsentwurf.

I. Allgemeine Bemerkungen

Das Bundesgericht ist bis auf ein paar Punkte mit dem Inhalt des vorgelegten Verordnungsentwurfs **einverstanden**.

Das Bundesgericht ist spezifisch durch die Definition der Formate (Art. 38e BGG) und das Inkrafttreten des Gesetzes (Art. 132b Abs. 2 BGG) sowie durch die Finanzierung der Plattform (Art. 32 und 33 BEKJ) betroffen.

II. Bemerkungen und Anregungen zu spezifischen Punkten

1. Ad Ingress VEKJ – Ergänzung mit BGG

Der Ingress sollte der Vollständigkeit halber mit dem Hinweis auf Art. 38e BGG ergänzt werden.

2. Ad Art. 2 Abs. 1 Bst. c VEKJ – Maximale Grösse der Dokumente

Die maximale Grösse der Dokumente wird auf zwei Gigabyte eingeschränkt. Die IT-Welt verändert sich im Eiltempo. Die Gesetzgebung auf Verordnungsebene nimmt Zeit in Anspruch, auch wenn es um einfache Nachführungen wie die Aufnahme von neuen technischen Angaben geht. Das Bundesgericht schlägt daher vor, dass die maximale Grösse der Dokumente nicht direkt in der Verordnung aufgeführt wird, sondern **in einem Anhang** an die VEKJ, der zum Beispiel in der Kompetenz des EJPD liegen würde.

3. Ad Art. 4 VEKJ – Format der Dokumente

a) Das Bundesgericht ist mit der vorgeschlagenen Lösung im Grundsatz einverstanden. Es ist insbesondere zu begrüssen, dass die meistverbreiteten Formate, die entgegengenommen werden müssen, im Voraus bekannt sind. Somit kann es sich auf den Empfang solcher Dateien vorbereiten.
b) Wie oben zu Art. 2 bereits begründet schlägt das Bundesgericht vor, dass die Liste der Formate von Art. 4 Abs. 3 VEKJ wiederum nicht direkt in der Verordnung aufgeführt wird, sondern in einem Anhang an die VEKJ (in der Kompetenz des EJPD).

4. Ad Art. 6 VEKJ – Siegelung der Dokumente

Behörden sind entweder Nutzer der Plattform im Sinne von Art. 22 Abs. 1 BEKJ (z. B. Gemeinden, die als Partei in einem Justizverfahren involviert sind) oder Verfahrensleitung im Sinne von Art. 22 Abs. 2 BEKJ. Das Obligatorium des Anbringens eines Siegels soll einzig für die Verfahrensleitung gelten. Wir schlagen deshalb vor, dies im Art. 6 VEKJ zu präzisieren: *«Übermittelt eine verfahrensleitende Behörde …»*. Die an einem Verfahren beteiligten Behörden sollen gleich wie die übrigen Verfahrensbeteiligten (Privatpersonen, Firmen, usw) behandelt werden.

5. Ad Art. 14 Abs. 2 VEKJ – Grösse der Dokumente bei der Virenprüfung

In dieser Bestimmungen wird eine Dateigrösse (64 MB) genannt. Mit der gleichen Begründung wie für die maximale Grösse der Dokumente und die Liste der Formate hier oben, schlägt das Bundesgericht vor, dass die Grösse der Dokumente nicht direkt in der Verordnung aufgefüllt wird, sondern in einem Anhang an die VEKJ, der in der Kompetenz des EJPD liegen würde.

6. Finanzierung (Art. 16 und 18 VEKJ)

Die Aufteilung zwischen dem EJPD und dem Bundesgericht (Art. 16 VEKJ) ist korrekt. Art. 18 VEKJ berücksichtigt die Kompetenzregelung zwischen dem Bundesgericht und den unterinstanzlichen Gerichten des Bundes und ist daher ebenfalls korrekt.

Wir danken Ihnen im Voraus für die Berücksichtigung unserer Bemerkungen und Anregungen.

Mit vorzüglicher Hochachtung

Der Generalsekretär

Nicolas Lüscher

Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Commission administrative

Viale Stefano Franscini 7
CH-6500 Bellinzone
Tel. +41 58 480 68 68
Fax +41 58 480 68 32
info@bstger.ch

Numéro d'enregistrement: 1.1.1.8

Département fédéral de justice et police
Office fédéral de la justice
Monsieur le Conseiller fédéral
Beat Jans
Palais fédéral ouest
3003 Berne

Par courrier électronique à
cornelia.perler@bj.admin.ch

Bellinzone, le 18 juin 2026/bom

Procédure de consultation
Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP) – prise de position

Monsieur le Conseiller fédéral,

Le Tribunal pénal fédéral vous remercie de l'occasion qui lui a été donnée de prendre position quant à l'objet susmentionné et se détermine comme suit.

En principe, le Tribunal pénal fédéral **approuve** le contenu du projet d'OCEP.

Le Tribunal salue en particulier le fait que le projet d'ordonnance définit d'emblée un certain nombre de formats de documents ; il nous semble cependant que pour tenir compte de l'évolution rapide des techniques, la taille maximum des documents (art. 2 al. 1 let. c OCEP), leurs formats (art. 4 OCEP) et la taille maximale des documents soumis à un contrôle antivirus (art. 14 al. 1 et 2 OCEP) devraient pouvoir être revus de manière plus souple que s'ils étaient d'ores et déjà fixés dans l'OCEP. Ils pourraient ainsi faire l'objet d'une annexe à l'OCEP et relever par exemple de la compétence du DFJP.

Veuillez agréer, Monsieur le Conseiller fédéral, l'expression de notre plus haute considération.

Roy Garré
Président

TRIBUNAL PENAL FEDERAL * BELLINZONE *

Marc-Antoine Borel
Secrétaire général

Copie à
- Tribunal fédéral
- Tribunal administratif fédéral
- Tribunal fédéral des brevets

Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Die Präsidentenkonferenz

Postfach, 9023 St. Gallen
Telefon +41 58 70 52727
Aktenzeichen: 111-30/22/5/2
Geschäfts-Nummer: 2026-063

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

PDF- und Word-Version per E-Mail an:

cornelia.perler@bj.admin.ch

St. Gallen, 10. Juni 2026 / geo

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ): Eröffnung des Vernehmlassungsverfahrens

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Für die Einladung vom 13. März 2026 zur Stellungnahme im eingangs erwähnten Vernehmlassungsverfahren danken wir. Den Entwurf haben wir mit Interesse zur Kenntnis genommen.

Das Bundesverwaltungsgericht nimmt wie folgt dazu Stellung:

Allgemeine Bemerkungen
Aus einer technologischen Sicht ist es für das Bundesverwaltungsgericht als nachgeordnete Beschwerdeinstanz wichtig, dass eine Vielzahl von technisch miteinander inkompatiblen Plattformlösungen möglichst zu vermeiden ist. Entsprechend ist nach Art. 25 Abs. 2 des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) die Interoperabilität der zentralen Plattform mit den anderen Plattformen Bewilligungsvoraussetzung. Es ist darauf zu achten, dass nicht nur die übermittelten Dokumente, sondern auch alle mit dem Datenaustausch verbundenen Daten – insbesondere Empfangsbestätigungen, Zeitstempel, Metadaten, Empfangsbestätigungen und Übertragungsinformationen – einheitlich definiert sind. Die für Schnittstellen und APIs der Plattformen verwendeten Technologien sollten gemeinsamen Standards entsprechen, um zu vermeiden, dass jede Behörde oder Fachanwendung spezifische Integrationen für mehrere verschiedene Plattformen entwickeln und warten muss, was langfristig einen erheblichen technischen und finanziellen Aufwand bedeuten würde. Wir gehen davon aus, dass diese Aspekte, wie es auf S. 6 im dritten Abschnitt im erläuternden Bericht festgehalten ist, in der geplanten Departementsverordnung adressiert werden.
Das Bundesverwaltungsgericht regt in diesem Sinne weiter an, einheitliche Regeln für die Benennung der über die Plattformen übermittelten Dokumente vorzusehen. Die Einführung einer gemeinsamen Namenskonvention würde die automatische Integration der Dokumente in die Fachanwendungen der verschiedenen Behörden erheblich erleichtern, manuelle Umbenennungen vermeiden und das Risiko von Fehlern, Doppelungen oder Informationsverlusten verringern. Dies könnte ebenfalls auf Stufe der Departementsverordnung geregelt werden.

Das Bundesverwaltungsgericht ruft zudem in Erinnerung, dass im Sozialversicherungsrecht mit dem Bundesgesetz über Informationssysteme in den Sozialversicherungen (BISS) geplant ist, eigene Wege zur elektronischen Beschwerdeführung mit einer elektronischen Plattform zu

schaffen. Es ist diesbezüglich sicherzustellen, dass keine Hindernisse und Doppelspurigkeiten bei den künftig elektronisch zu führenden verwaltungsgerichtlichen Verfahren im Sozialversicherungsrecht entstehen.

Zu Art. 2 Abs. 1 Bst. c VE-VEKJ

Im erläuternden Bericht (S. 11) werden in den Abschnitten 3-5 Dateien behandelt, deren Grösse zwei Gigabyte übersteigt. Der Text der Verordnung schliesst nicht aus, dass Plattformen solche Dateien entgegennehmen und übermitteln können. Müssten beispielsweise Dateien eines beschlagnahmten Computers in hunderte von Teilen aufgespalten werden, könnten sich Fragen im Zusammenhang mit dem Authentizitätsnachweis stellen. Es könnte sich als sinnvoll erweisen, den Plattformen unter gewissen Umständen die Entgegennahme und Weiterleitung grösserer Dateien vorzuschreiben. In diese Richtung deutet auch der Bericht («Damit solche Abbilder und Dateien übermittelt werden können, ohne in mehrere Teile aufgespalten zu werden, können Betreiberinnen von Plattformen auch die Übermittlung von grösseren Dokumenten durch spezifische Benutzerinnen und Benutzer zulassen»).

Dass die Einwilligung (wohl der Plattformbetreiberinnen und -betreiber gegenüber spezifischen Benutzerinnen und Benutzern) für die Übermittlung grösserer Datenmengen mündlich oder schriftlich erfolgen können soll, wird in der Verordnung nicht erwähnt.

Der sechste Abschnitt im erläuternden Bericht erscheint unklar, zumal diese Aussage (wie der Inhalt der Abschnitte 3-5) dem Normtext der Verordnung nicht entnommen werden kann. Es ist unklar, wer den Zugriff auf eine forensische Applikation erlauben kann und welchen Anforderungen eine solche Applikation genügen müsste. Es wäre wohl anzunehmen, dass es die im BEKJ geregelten Plattformen sind.

Insgesamt ist festzuhalten, dass im erläuternden Bericht zu Art. 2 Abs. 1 Bst. c VE-VEKJ einige Aspekte erwähnt sind, die sich aus der Verordnung nicht ergeben.

Zu Art. 2 Abs. 1 Bst. d VE-VEKJ

In der Verordnung sollte präzisiert werden, dass die Dokumente und Quittungen «aus ihrem Konto» gelöscht werden können. So wird deutlich, dass die Dateien andernorts noch hinterlegt sein können. Je nach Art des Dokuments wird es nie endgültig gelöscht, sondern archiviert.

Zu Art. 3 Abs. 2 VE-VEKJ

Es wird nur auf die Voraussetzungen nach Art. 2 (VE-VEKJ) verwiesen. Damit eine Bewilligung erteilt werden kann, müssen aber auch weitere Anforderungen nach dem BEKJ erfüllt sein. In Art. 3 Abs. 4 VE-VEKJ wird in Bezug auf den Entzug einer Bewilligung zusätzlich zu Art. 2 VE-VEKJ auch auf Art. 25 BEKJ (der seinerseits in Abs. 2 auf den 3. Abschnitt des BEKJ und weitere Bestimmungen verweist) verwiesen. Dieser Verweis wäre bereits in Abs. 2 von Art. 3 des VE-VEKJ sinnvoll.

Die im erläuternden Bericht genannten Voraussetzungen finden sich weder im VE-VEKJ noch im BEKJ. Es fehlt beispielsweise der Hinweis, dass eine Betreiberin ein Konzept vorlegen müsse, welches belegt, dass sämtliche Bewilligungsvoraussetzungen erfüllt sind. Der Nachweis, dass die Bewilligungsvoraussetzungen erfüllt sind, müsste – gestützt auf BEKJ und VE-VEKJ – auch auf andere Weise als durch ein Konzept möglich sein.

Zu Art. 3 Abs. 4 VE-VEKJ

Im Zusammenhang mit dem Bewilligungsentzug stellt sich die Frage, was mit den Daten (insbesondere jenen der Benutzer) geschieht, wenn einer Betreiberin eine Bewilligung entzogen wird oder wenn sie in Konkurs fallen sollte.

Zu Art. 3 Abs. 5 VE-VEKJ

Diese Norm regelt die Höhe der Gebühren. Die Norm ist aber nicht abschliessend, denn es gilt auch die AllGebV. Es wäre sinnvoll, in der Verordnung selbst auf die Anwendung der AllGebV

hinzuweisen und nicht erst im erläuternden Bericht (ebenso Art. 16 VE-VEKJ). Art. 3 Abs. 5 VE-VEKJ könnte sonst als abschliessende Regelung angesehen werden.

Zu Art. 4 Abs. 2 VE-VEKJ
Im erläuternden Bericht (S. 14) steht, dass das Risiko, ob eine Behörde die Beilage öffnen und verwenden könne, grundsätzlich bei der Absenderin oder beim Absender liege. Das ergibt sich aber weder aus dem BEKJ noch dem VE-VEKJ. Art. 4 Abs. 2 i.V.m. Abs. 4 und 5 VE-VEKJ deutet insofern in eine andere Richtung, als die Behörde der Absenderin oder dem Absender eine angemessene Frist einräumen muss, damit sie oder er die Beilagen in geeigneter Weise einreichen kann. Mit Verweis auf die Rechtssicherheit erschiene eine entsprechende Präzisierung sinnvoll.

Zu Art. 4 Abs. 4 VE-VEKJ
Der letzte Teilsatz von Art. 4 Abs. 4 VE-VEKJ («den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen») erscheint unklar. Es stellt sich die Frage, ob die Behörde selbst festlegt, wie dies zu geschehen hat.

Zu Art. 5 Abs. 1 VE-VEKJ
Vorschlag für die Formulierung: «[E]ine ***einzige*** Quittung» statt «eine einzelne Quittung», wenn gemäss erläuterndem Bericht (S. 17) ausgesagt werden soll, dass eine Quittung für mehrere Dokumente genügt und nicht für jedes einzelne Dokument eine ausgestellt werden muss.

Zu Art. 5 Abs. 2 Bst. d Ziff. 1 VE-VKJ
Um klarzustellen, dass Grösse und Hashwert von jedem Dokument separat angegeben werden müssen, wie im erläuternden Bericht (S. 17) steht, könnte vor «Grösse» und «Hashwerte» «jeweilige» bzw. «jeweils» eingesetzt werden, also: «deren ***jeweilige*** Grösse und die ***jeweils*** dazugehörigen Hashwerte».

Zu Art. 6 VE-VEKJ
Dieser Artikel sieht vor, dass es ausreicht, wenn nur *eines* der Dokumente über Siegel und Zeitstempel verfügt, sofern eine Behörde mehrere Dokumente zusammen an eine Plattform übermittelt. Art. 22 Abs. 2 BEKJ hält aber fest, dass die Behörden *die* Dokumente mit Siegel und Zeitstempel versehen muss und die Plattform die Dokumente sonst nicht entgegennimmt. Diesbezüglich scheint ein Widerspruch zu bestehen.

Zu Art. 7 VE-VEKJ
Es wäre sinnvoll zu regeln, dass Art. 6 und 7 VE-VEKJ nicht für die Akteneinsicht gelten. Das im erläuternden Bericht (S. 19) zur Akteneinsicht Ausgeführte ergibt sich nicht aus dem Gesetz. Im Bericht steht, aus Art. 22 BEKJ ergebe sich e contrario, dass für die Akteneinsicht kein Siegel anzubringen sei. Auch bei den Dateien für die Akteneinsicht handelt es sich aber um Dokumente, die einer Zustellung bedürfen. In der Regel werden die Akten mit einer Verfügung zugänglich gemacht werden, in der auch eine Frist zur Stellungnahme angesetzt wird. Diese Verfügung wird dann mit Siegel und Zeitstempel zu versehen sein. Weder Gesetz noch Verordnung halten aber fest, dass auf jenen Dokumenten, in die Akteneinsicht gewährt wird, kein Siegel und kein Zeitstempel angebracht werden müssen.

Zu Art. 12 Abs. 1 VE-VEKJ
Nach dieser Vorschrift sind die auf der Plattform gespeicherten Dokumente und Quittungen sechs Monate nach Entgegennahme bzw. nach Erstellung automatisch zu vernichten. Im erläuternden Bericht wird auf S. 23 präzisiert, dass diese Vernichtung innerhalb von 24 Stunden nach Ablauf der sechs Monate erfolgen muss. Das Bundesverwaltungsgericht regt an, diese spezifische Vorgabe auch in der Verordnung zu verankern.

Zu Art. 14 Abs. 2 und 4 VE-VEKJ
Wird ein Dokument aufgrund seiner Grösse für die Virenprüfung in verschiedene Teile aufgespalten, muss das Dokument entsprechend gekennzeichnet werden. Gemäss dem erläuternden Bericht (S. 25) kann so die Empfängerin oder der Empfänger die «notwendige Sorgfalt» walten lassen. Dieser Begriff bedürfte allenfalls weiterer Präzisierung.

Zu Art. 14 Abs. 3 VE-VEKJ
Beim BVGer dürfte es selten vorkommen, dass Dokumente mit Schadsoftware eingereicht werden müssen. Dennoch erscheint es heikel, dass ein entsprechender Auftrag, von der Virenscannung abzusehen, *mündlich* erteilt werden kann. Es stellt sich deshalb die Frage, wie die Person identifiziert wird, die den Auftrag erteilt.

Zu Art. 15 Abs. 5 VE-VEKJ
Der erläuternde Bericht hält fest, dass bereits im geltenden Prozessrecht geregelt ist, wie mit Dokumenten umzugehen ist, welche Schadsoftware enthalten. Es stellt sich die Frage, wie damit umzugehen ist, wenn es sich um eine Beschwerde mit Schadsoftware handelt, die im letztmöglichen Zeitpunkt aufgegeben wird. Gilt sie dann, weil sie zurückgewiesen wird, bei Neueinreichung als verspätet, weshalb darauf nicht eingetreten wird, oder gilt sie als mangelhaft, weshalb eine Nachfrist angesetzt wird? Das Bundesverwaltungsgericht würde eine Klärung dieses Punktes begrüssen.

Im Übrigen verzichtet das Bundesverwaltungsgericht auf eine Stellungnahme.

Freundliche Grüsse

Die Vorsitzende der Präsidentenkonferenz	Der stellvertretende Generalsekretär
Barbara Balmelli	Bernhard Fasel

Kopie an

- Bundesgericht
- Bundesstrafgericht
- Bundespatentgericht

Conférence latine des Chefs des Départements de justice et police (CLDJP)
Conférence latine des Chefs des Départements compétents en matière d'asile et des migrants (CLDAM)
Conférence latine des Directrices et Directeurs des affaires militaires et de la protection de la population (CLAMPP)

Par e-mail (cornelia.perler@bj.admin.ch)
Monsieur le Conseiller fédéral
Beat Jans
Département fédéral de justice et police

Fribourg, le 7 avril 2026

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP) : consultation

Monsieur le Conseiller fédéral,

Les membres de la Conférence latine des chefs des départements de justice et police (CLDJP) vous remercient de les avoir consultés sur l'objet cité en titre.

Après en avoir débattu lors de sa séance du printemps 2026, la Conférence souhaite vous sensibiliser à un aspect particulier du projet.

Les cantons latins saluent la volonté de la Confédération de réaliser la transition numérique de la justice par le biais de la Loi sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ). L'obligation de tenir le dossier judiciaire sous forme électronique (art. 100 al. 3 nCPP) constitue une avancée majeure vers une justice plus moderne et efficiente. Toutefois, la mise en œuvre pratique de cette loi ne doit pas générer de charges administratives disproportionnées qui iraient à l'encontre du but recherché par le législateur.

Un point de préoccupation majeur réside dans l'interprétation des dispositions du Code de procédure pénale (CPP) relatives à la notification des prononcés (notamment les art. 80 al. 2 et 353 al. 1 let. k CPP). Sans une clarification explicite dans l'ordonnance d'application, les ministères publics et services administratifs pourraient être contraints de signer manuellement des dizaines de milliers d'ordonnances chaque année avant leur envoi postal ; il en résulte un risque de grande surcharge administrative, sans aucun gain de qualité de la prestation. Nous rejoignons donc l'interprétation défendue par le projet Justitia 4.0 et le Tribunal fédéral : dès lors que la décision originale électronique est signée et versée au dossier, sa notification par voie postale doit pouvoir se faire par une copie papier dépourvue de signature manuscrite.

Nous demandons donc que l'ordonnance d'application intègre les principes suivants :

- **Reconnaissance de la copie papier** : l'envoi postal d'une copie papier de la décision originale électronique doit être considéré comme une notification valable pour les parties qui ne communiquant pas par voie électronique (art. 103c et 103d nCPP).
- **Déclenchement des délais** : il doit être expressément prévu que cette notification papier déclenche les délais légaux d'opposition, d'appel ou de recours.
- **Sécurité juridique** : cette solution assure la pérennité des processus déjà en place dans plusieurs cantons tout en garantissant l'authenticité de l'acte par le dossier électronique original.

L'entrée en vigueur complète de la LPCJ doit marquer une étape de simplification et non un retour à des contraintes formelles obsolètes. Les départements de justice des cantons latins soutiennent fermement l'introduction d'une disposition claire dans l'OCEP permettant la notification de copies papier issues d'originaux électroniques sans exigence de signature manuscrite additionnelle.

Le soussigné de droite se tient à votre disposition pour tout complément.

Nous vous remercions de bien vouloir prendre en compte cette demande et vous prions de croire, Monsieur le Conseiller fédéral, à l'assurance de notre considération distinguée.

Le président	Le secrétaire général
Romain Collaud Conseiller d'Etat	Christian Clerici

HIS SCHWEIZ
HIJP SUISSE
AIGP SVIZZERA

Per E-Mail:
Bundesamt für Justiz

cornelia.perler@bj.admin.ch

Bern, 22. Juni 2026

Vernehmlassung VEKJ 2026: Stellungnahme HIS Schweiz

Sehr geehrter Herr Bundesrat
Geschätzte Damen und Herren

Wir bedanken uns sehr für die Gelegenheit im Rahmen der Vernehmlassung VEKJ (Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren) Stellung nehmen zu dürfen.

Ebenso bedanken wir uns dafür, dass wir im Rahmen der Begleitgruppe VBEKJ zu den Vorversionen konstruktiv beitragen durften.

Sie finden unsere Anmerkungen zur aktuellen Version aus Sicht von HIS Schweiz auf den nächsten Seiten. Sie sind auf vier, unserer Meinung nach, wichtige thematische Hauptpunkte fokussiert. Im Übrigen unterstützen wir die Vernehmlassung von Justitia 4.0.

Sehr gerne stehen wir für Rückfragen zur Verfügung.

Freundlich grüssen

HIS Schweiz

Dr. Jens Piesbergen
Direktor

Albano Bernasconi
Leiter Technologie und Innovation

Inhaltsverzeichnis

Zusammenfassung der thematischen Anliegen dieser Stellungnahme 2

1 Titel der Verordnung: Anpassung 3

2 Art. 1 Abs. 1: Ergänzung 4

3 Art. 4 Format der Dokumente: Präzisierung des Geltungsbereichs und Delegation der Regelungskompetenz 4

4 Art. 4 Format der Dokumente: zusätzlicher neuer Artikel zu strukturierten Verfahrensdaten 5

5 Art. 8 Authentifizierung der Benutzerinnen und Benutzer: Delegation der Regelungskompetenz 6

6 Art. 9 Profile: Streichung Postadresse 6

7 Art. 23 Eignungsvoraussetzung und Art 24 Elektronische Übermittlung unter Behörden: Zusammenlegung und Präzisierung 6

Zusammenfassung der thematischen Anliegen dieser Stellungnahme

Die Kapitel 1 und 2 betreffen die Erweiterung des Anwendungsbereichs der Verordnung. Vorgeschlagen wird, den Titel der VEKJ nicht nur auf bundesrechtliche Verfahren zu beschränken und Art. 1 Abs. 1 um eine Grundlage für eine künftige Anbindung kantonaler Verwaltungsverfahren, insbesondere im Justizvollzug als Teil der Strafjustizkette, zu ermöglichen.

Die Kapitel 3 und 4 behandeln die technischen Grundlagen für Dokumente und strukturierte Verfahrensdaten. Einerseits soll Art. 4 präzisieren, dass die Vorgaben zu Dateiformaten sowohl für Übermittlungen über Plattformen als auch ausserhalb einer Plattform nach BEKJ gelten. Andererseits soll ein neuer Artikel zu strukturierten Verfahrensdaten geschaffen werden, damit maschinenlesbare Daten in anerkannten Formaten, insbesondere nach eCH-Standards, ausdrücklich genutzt und übermittelt werden sollen.

Die Kapitel 5 und 6 betreffen die Benutzerinnen und Benutzer der Plattform. Bei der Authentifizierung wird AGOV als zweckmässige Lösung unterstützt; die erforderliche Authentifizierungsqualität soll jedoch durch das EJPD näher geregelt werden. Bei den Profilangaben soll insbesondere auf die Postadresse verzichtet werden, da sie für die elektronische Zustellung keinen Mehrwert bietet und datenschutzrechtlich kritisch sein kann.

Kapitel 7 befasst sich mit der elektronischen Übermittlung unter Behörden nach Art. 23 und 24. HIS Schweiz schlägt vor, die beiden Bestimmungen zusammenzulegen und zu präzisieren, damit sichere technische Lösungen für den Austausch mit allen Verfahrensbeteiligten wie auch dem zwischenbehördlichen Verkehr klar geregelt werden. Dabei soll insbesondere festgehalten werden, unter welchen Voraussetzungen solche Lösungen keiner Bewilligungspflicht unterliegen und wie deren Eignung nachzuweisen ist.

1 Titel der Verordnung: Anpassung

Der Titel der Verordnung ist neu zu formulieren mit:

> *Verordnung über die elektronische Kommunikation in ~~bundesrechtlichen~~ Justiz- und Verwaltungsverfahren (VEKJ)*

Begründung: Im Rahmen der Umsetzung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation (BEKJ) sowie der dazugehörigen Verordnung (VEKJ) stellt sich die Frage, ob es erforderlich ist, auch Bestimmungen vorzusehen, welche die Nutzung der Plattform für kantonale Verwaltungsverfahren ausserhalb des Justizbereichs ermöglichen. Dies mit dem strategischen Gedanken, dass wenn der Bund mit seinem eigenen verwaltungsrechtlichen Anliegen auf die VEKJ einwirkt, auch die Kantone mit gutem Recht analog argumentieren sollten. Immerhin sind die Kantone wichtige Stakeholder, die durchaus ihre Anliegen beisteuern sollten.

Rechtlicher Hintergrund: Ausgangspunkt bildet dabei die Zielsetzung des BEKJ, den elektronischen Rechtsverkehr zwischen Behörden und Verfahrensbeteiligten umfassend zu regeln und langfristig eine durchgehend digitale Abwicklung staatlicher Verfahren zu ermöglichen. Dies beschränkt sich nicht allein auf klassische Gerichtsverfahren, sondern umfasst auch Verwaltungsverfahren, welche einen erheblichen Teil staatlicher Tätigkeit ausmachen. So sieht das Gesetz ausdrücklich vor, dass für Verwaltungsverfahren des Bundes eine eigene Plattform bereitgestellt wird (vgl. Art. 6a Abs. 2 VwVG, der durch eine Drittänderung des BEKJ erlassen wurde). Bereits daraus ergibt sich, dass der elektronische Rechtsverkehr nicht auf den Justizbereich beschränkt ist, sondern systematisch auch Verwaltungsprozesse einbezieht. Eine systematische Auslegung bestätigt dieses Verständnis.

Die VEKJ ist so konzipiert, dass sie für sämtliche Plattformen nach BEKJ sowie für weitere Plattformen gilt, soweit diese in den Anwendungsbereich des Gesetzes fallen (Art. 1 Abs. 1 und 2 VE-VEKJ). Der Gesetzgeber hat den Regelungsbereich somit bewusst offen und plattformübergreifend gestaltet. Würden kantonale Verwaltungsverfahren im nicht justiziellen Bereich von dieser Systematik ausgeschlossen, entstünden parallele Kommunikationssysteme mit unterschiedlichen technischen und rechtlichen Standards. Dies würde dem Ziel eines einheitlichen elektronischen Rechtsverkehrs zuwiderlaufen und die angestrebte Harmonisierung untergraben. Auch die teleologische Auslegung führt zu diesem Ergebnis.

Ziel des BEKJ ist es ausdrücklich, durchgängig digitale und medienbruchfreie Verfahren zu ermöglichen. Dieses Ziel kann nur erreicht werden, wenn sämtliche relevanten staatlichen Verfahren in die digitale Infrastruktur integriert werden. Eine Beschränkung auf gerichtliche Verfahren würde zwangsläufig dazu führen, dass zwischen Verwaltungs- und Justizverfahren weiterhin Medienbrüche bestehen, etwa wenn ein Verfahren von einer Verwaltungsbehörde zu einem Gericht weitergezogen wird. Die Effizienzgewinne der Digitalisierung könnten in einem solchen Fall nur teilweise realisiert werden.

Besonders ins Gewicht fällt zudem der föderalistische Aufbau der Schweiz. Verwaltungs- und Rechtsmittelverfahren verlaufen häufig über mehrere Ebenen hinweg, insbesondere zwischen kantonalen Behörden und Bundesinstanzen. Ohne Einbezug der kantonalen Verwaltungsverfahren bestünde die Gefahr von Schnittstellenproblemen, welche den Datenaustausch erschweren und den Verfahrensablauf verkomplizieren könnten. Eine gemeinsame Plattform trägt hingegen wesentlich zur Interoperabilität bei und gewährleistet kohärente Abläufe über alle Staatsebenen hinweg.

Schliesslich sprechen auch praktische und wirtschaftliche Überlegungen für eine entsprechende Ausweitung. Der Betrieb der zentralen Plattform verursacht erhebliche Kosten von rund 10 bis 12 Millionen Franken pro Jahr. Vor diesem Hintergrund ist es sachgerecht, die Infrastruktur möglichst umfassend zu nutzen, um Effizienz- und Skaleneffekte zu erzielen. Die Einbeziehung kantonaler Verwaltungsverfahren erhöht die Auslastung der Plattform und trägt damit zur wirtschaftlichen Rechtfertigung des Systems bei. Hinzu kommt ein Aspekt der Nutzerfreundlichkeit und Gleichbehandlung. Für Bürgerinnen und Bürger sowie Unternehmen ist es von zentraler Bedeutung, mit Behörden über einen einheitlichen Kommunikationskanal interagieren zu können. Müssten je nach Verfahren unterschiedliche Systeme oder Kommunikationswege genutzt werden, würde dies die Komplexität erhöhen und die Akzeptanz der Plattform beeinträchtigen. Eine umfassende Einbindung auch der kantonalen Verwaltungsverfahren trägt demgegenüber zu einer konsistenten und niederschwelligen Nutzung bei.

Zusammenfassend ergeben systematische, teleologische, föderalistische sowie praktische Überlegungen, dass es notwendig ist, bei der Umsetzung von BEKJ und VEKJ auch spezifische Bestimmungen vorzusehen, welche die Nutzung der Plattform für kantonale Verwaltungsverfahren ausserhalb des Justizbereichs ermöglichen. Dies gilt insbesondere im Hinblick auf die Einführung einer eJVAkte, die je nach Ausgestaltung gewisse Besonderheiten gegenüber dem bundesrechtlichen Verwaltungsverfahren aufweisen oder voraussetzen kann. Ohne eine solche Einbindung würde das gesetzgeberische Ziel eines einheitlichen und durchgängig digitalen Rechtsverkehrs verfehlt, während wesentliche Effizienz- und Koordinationsgewinne ungenutzt blieben.

Vorerst erscheint es ausreichend, wenn in der VEKJ zumindest die Anbindungsmöglichkeit der Kantone klar verankert wird (siehe Art. 1 Abs. 1 lit. d)

2 Art. 1 Abs. 1: Ergänzung

Analog lit. c ist eine lit. d einzuführen, welche zugunsten kantonaler Verwaltungsverfahren, insbesondere des Justizvollzugs als Teil der sog. Strafjustizkette, verweist mit:

> *d geplante interkantonale Plattform für den Justizvollzug*

Begründung: Dies ist ein juristisches *whitelabel* von justitia.swiss zugunsten des Justizvollzugs analog lit. c. auf Stufe Bund für seine zukünftige Plattform für die Verwaltungsverfahrens des Bundes. Weitere Erläuterungen gemäss Ausführungen zu «Titel der Verordnung» (s.o.).

3 Art. 4 Format der Dokumente: Präzisierung des Geltungsbereichs und Delegation der Regelungskompetenz

Art. 4 des Vorentwurfs regelt die Anforderungen an die Formate von Dokumenten bzw. Dateien im elektronischen Rechtsverkehr und legt damit eine zentrale Grundlage für eine effiziente, sichere und medienbruchfreie Aktenführung fest. Die Vorgaben zielen darauf ab, die Interoperabilität zwischen den Verfahrensbeteiligten zu gewährleisten und die Bearbeitbarkeit der eingereichten Unterlagen sicherzustellen. Die Festlegung von verbreiteten und technisch stabilen Formaten ist zu begrüssen, da sie die Arbeitsabläufe vereinfacht, Konvertierungsaufwände reduziert und die IT-Sicherheit erhöht.

Gleichzeitig erfordern der technische Fortschritt und die Vielfalt digitaler Inhalte eine gewisse Flexibilität bei der Wahl der Dateiformate. Nicht alle Inhalte lassen sich in klassischen Formaten wie PDF adäquat abbilden. Daher ist es wesentlich, neben klar definierten Standardformaten auch Ausnahmen vorzusehen und technische Detailregelungen auf einer anpassungsfähigen Normstufe zu verankern, um ein ausgewogenes Verhältnis zwischen Standardisierung und technologischer Offenheit sicherzustellen.

Vorschlag: Der Artikel «Format der Dokumente» soll ausdrücklich die Formate zur Übermittlung über die Plattform und ausserhalb einer Plattform nach dem BEKJ gleichermassen regeln. Die Kompetenz zur genaueren Regelung der übertragbaren Dateiformate soll dem EJPD übertragen werden

> *Art. 4 Format der Dokumente*
> *[1] Die verfahrensleitenden und die verfahrensbeteiligten Behörden erstellen ihre Dokumente zur Übermittlung über die Plattformen oder ausserhalb einer Plattform nach dem BEKJ im Format PDF/A, die übrigen Verfahrensbeteiligten im Format PDF oder PDF/A.*
> *[2] Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, soll stattdessen eine Datei als Beilage im Originalformat übermittelt werden.*
> *[3] Kann die verfahrensleitende Behörde eine Beilage im Format, in dem sie eingereicht wurde, nicht öffnen, so räumt sie der einreichenden Partei eine angemessene Frist ein, damit diese die Beilage in einem von der Behörde festgelegten Format einreichen kann.*
> *[4] Das EJPD regelt die über die Plattformen und ausserhalb einer Plattform nach dem BEKJ übertragbaren Dateiformate.*

Erläuterungen:
- Absatz 1 bestimmt die verbindlichen Dateiformate für die Erstellung und Übermittlung von Dokumenten für alle Beteiligten, unabhängig davon, ob die Übermittlung über die Plattformen oder ausserhalb einer Plattform nach dem BEKJ stattfindet.
- Absatz 2 regelt die praxisorientierte Ausnahme für Inhalte, die im PDF-Format nicht korrekt oder vollständig dargestellt werden können (z. B. bei komplexen Datensätzen oder Medienformaten). In diesen Fällen soll das Originalformat als Beilage mitübermittelt werden.
- Im Absatz 3 wird der Umgang mit technischen Problemen bei der Verarbeitung von Beilagen geregelt. Kann die verfahrensleitende Behörde eine eingereichte Datei nicht öffnen, muss sie der einreichenden Partei eine angemessene Frist einräumen, um die Beilage in einem geeigneten Format erneut einzureichen.
- Absatz 4 überträgt die Regelungskompetenz für zulässige Dateiformate dem EJPD. Das Departement legt in einer Verordnung fest, welche Formate verwendet werden dürfen. Dadurch wird eine einheitliche und anpassungsfähige Festlegung technischer Standards ermöglicht.

4 Art. 4 Format der Dokumente: zusätzlicher neuer Artikel zu strukturierten Verfahrensdaten

Die Digitalisierung des elektronischen Rechtsverkehrs soll Verfahren effizienter, schneller und qualitativ hochwertiger machen. Dies setzt voraus, dass neben menschenlesbaren Dokumenten auch strukturierte, maschinenlesbare Verfahrensdaten genutzt und zuverlässig zwischen Behörden, Plattformen und Verfahrensbeteiligten ausgetauscht werden können.

Strukturierte Verfahrensdaten ermöglichen automatisierte Weiterverarbeitung, reduzieren Medienbrüche und vermeiden Übertragungsfehler. Die bisherigen Regelungen fokussieren jedoch primär auf Dokumente und erfassen strukturierte Daten nicht ausdrücklich als eigenständige Kategorie. Deshalb braucht es klare Vorgaben zu Zulässigkeit, Formaten und Weiterverwendung; eine Übermittlungspflicht soll nur für bereits vorhandene Daten gelten, soweit dies technisch möglich und zumutbar ist.

Vorschlag: Ein neuer Artikel «Strukturierte Verfahrensdaten» soll die Kompetenz des EJPD zur Regelung der Dateiformate für strukturierte Verfahrensdaten ausdrücklich festhalten und präzisieren. Die Pflicht zur Übermittlung strukturierter Verfahrensdaten soll auf bereits vorhandene Daten beschränkt werden und unter dem Vorbehalt der technischen Möglichkeit und Zumutbarkeit stehen.

> *Art. 4a Strukturierte Verfahrensdaten*
> *[1] Das EJPD regelt insbesondere die Dateiformate für die Übermittlung von strukturierten Verfahrensdaten über die Plattformen oder ausserhalb einer Plattform nach dem BEKJ. Es kann dazu verbindliche Vorgaben festlegen und auf anerkannte Standards, namentlich eCH-Standards, verweisen.*
> *[2] Die verfahrensleitenden Behörden und die Verfahrensbeteiligten sind verpflichtet, bereits vorhandene strukturierte Verfahrensdaten in den bezeichneten Dateiformaten zu übermitteln, soweit ihnen dies technisch möglich und zumutbar ist.*

Erläuterungen:
- Absatz 1 überträgt dem EJPD die Kompetenz, die zulässigen Dateiformate für strukturierte Verfahrensdaten zu bezeichnen. Die Regelung gilt sowohl für die Übermittlung über die Plattformen als auch für die Übermittlung ausserhalb einer Plattform nach dem BEKJ.
- Das EJPD kann verbindliche technische Vorgaben erlassen und dabei auf anerkannte Standards, insbesondere eCH-Standards, verweisen. Dadurch wird eine schweizweit einheitliche und interoperable Datenübermittlung unterstützt.
- Absatz 2 begrenzt die Pflicht zur Übermittlung strukturierter Verfahrensdaten auf Fälle, in denen solche Daten bereits vorhanden sind und ihre Übermittlung technisch möglich sowie zumutbar ist. Damit wird verhindert, dass Verfahrensbeteiligte zur nachträglichen Erstellung strukturierter Daten verpflichtet werden.

5 Art. 8 Authentifizierung der Benutzerinnen und Benutzer: Delegation der Regelungskompetenz

Die Authentifizierung über AGOV gemäss Absatz 1 ist sinnvoll und zielführend. Die detaillierten Anforderungen sollten in einer Departementsverordnung des EJPD geregelt werden:

Vorschlag:

> *Art. 8 Authentifizierung der Benutzerinnen und Benutzer*
> *[1] Für die Authentifizierung der Benutzerinnen und Benutzer der Plattformen nach Artikel 1 Buchstaben a und c sowie einer vom Bund zur Verfügung gestellten Plattform nach Artikel 1 Buchstabe b wird das System «AGOV» nach Artikel 11 Absatz 3bis des Bundesgesetzes vom 17. März 2023 über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben verwendet.*
> *[2] Das EJPD regelt die erforderliche Authentifizierungsqualität.*

Der mögliche Einsatz von zusätzlichen Authentifizierungsdiensten bei künftigen kantonalen Plattformen gemäss Absatz 2 wird begrüsst. Künftig sind die meisten Behörden über eine Schnittstelle mit der zentralen Plattform verbunden. Absatz 3 lässt genügend Spielraum, um künftige technische Lösungen umzusetzen.

6 Art. 9 Profile: Streichung Postadresse

Art. 9 Abs. 2 und 3: Für alle Teilnehmer, also für verfahrensleitende Behörden sowie für natürliche Personen und Organisationen, ist auf die Angabe einer Postadresse zu verzichten, da diese aufgrund mehrerer Standorte, fehlender Aktualität und fehlender Überprüfung keine verlässliche Information darstellt und für die elektronische Zustellung keinen Mehrwert bietet; zudem ist ihre Speicherung aus datenschutzrechtlicher Sicht kritisch zu beurteilen.

HIS Schweiz begrüsst die Möglichkeit, zusätzliche Informationen als die in der Verordnung angegebenen in den Benutzerprofilen zu führen, die der Wortlaut des Artikels ("mindestens folgende Angaben") ausdrücklich bietet. Wir denken dabei insbesondere an Angaben zu Verarbeitungsfähigkeiten von bestimmten Formaten von strukturierten Verfahrensdaten pro teilnehmende Stelle.

Im Übrigen unterstützen wir für die Formulierung des Artikels 9 die Stellungnahme von Justitia 4.0.

7 Art. 23 Eignungsvoraussetzung und Art 24 Elektronische Übermittlung unter Behörden: Zusammenlegung und Präzisierung

Unsere Bemerkungen zu Art. 23 und 24 sind im Folgenden zweiteilig. Schliesslich führen sie dazu, dass wir empfehlen

- eine Zusammenlegung der beiden Artikel vorzunehmen, da nicht unterschieden werden soll, ob unterschiedliche Kriterien für einen Austausch unter Behörden oder mit Verfahrensbeteiligten gelten sollen.
- Auf alle Fälle sind Präzisierungen vorzunehmen.

Begründung: «Andere Zustellplattformen» gemäss Art. 4 BEKJ unterliegen dem Vorbehalt der Bewilligung durch das EJPD. Art. 103b Abs. 1 StPO sieht vor, dass eine Strafbehörde (Art. 12 StPO) die Akten über eine Plattform nach BEKJ weitergeben sollen.

Unter Einhaltung der Voraussetzungen von Art. 103b Abs. 2 lit. a und lit. b StPO, die nun in Art. 23 VEKJ konkretisiert sind, können auch andere Lösungen eingesetzt werden. Demnach ist die Übermittlung unter Strafbehörden auch erlaubt, wenn der Zeitpunkt der Übermittlung festgehalten wird (lit. a), ein synchronisierter Zeitstempel verwendet wird (lit. b) und die Akten bei der Übermittlung und in der Ablage vor Veränderung und unberechtigter Kenntnisnahme geschützt ist (lit. c). Sind diese Voraussetzungen nach Art. 23 VEKJ erfüllt, ist die Verwendung von «anderen Lösungen» zur Übermittlung von Dokumenten unter Strafbehörden möglich (Erläuternder Bericht, S. 32).

Viele Polizeikorps oder andere Behörden liefern ihre Akten direkt über eine sichere Schnittstelle in die Fachapplikation einer Staatsanwaltschaft ein. Diese Art der Übermittlung erfüllt bereits heute die Voraussetzungen von Art. 23 VEKJ. Es herrscht Uneinigkeit darüber, ob die beschriebene innerkantonale Übermittlungsart zwischen Polizei und Staatsanwaltschaft (resp. anderen Behörden) eine Bewilligungspflichtige im Sinne von Art. 1 ff. VEKJ darstellt. Dazu besteht in der Verordnung eine Lücke, welche geschlossen werden sollte.

Im Weiteren wird in den Prozessgesetzen, bspw. der StPO, für den elektronischen Rechtsverkehr von zwei unterschiedlichen Fällen ausgegangen, je nachdem, welche Beteiligten involviert sind: einerseits vom Verkehr zwischen den Behörden der Verfahrenskette und andererseits vom Verkehr zwischen verfahrensleitenden und beteiligten Behörden. Falls eine solche Unterscheidung zwingend notwendig sein sollte, ist diese hinreichend zu präzisieren, da beim Lesen der VEKJ die Unterscheidungen in den Verfahrensgesetzen nicht präsent ist, andernfalls ist in der VEKJ eine Regelung vorzusehen, die für alle geeigneten Übermittlungslösungen ausserhalb der Plattformen dieselben Kriterien anwendet.

Vorgeschlagene Lösung (zusammengelegte Art. 23/24)

> *Art 23 Eignungsvoraussetzungen für andere Übermittlungslösungen*
> *[1] In Umsetzung von Artikel 128b Absatz 3 und Artikel 128c Absatz 2 ZPO, Artikel 103b Absatz 3 und Artikel 103c Absatz 2 StPO sowie Artikel 8c Absatz 3 und Artikel 8d Absatz 2 OHG können für die Weitergabe bzw. Übermittlung der elektronischen Akten zwischen Behörden des gleichen Kantons sowie zwischen Strafbehörden auch andere technische Lösungen eingesetzt werden.*
> *[2] Solche Lösungen sind für die Übermittlung geeignet, wenn sie erlauben:*
> *a. die Zeitpunkte der Übermittlung eindeutig festzustellen; und*
> *b. die Dokumente bzw. Dateien vor Veränderung und unberechtigter Kenntnisnahme zu schützen.*
> *[3] Für die Übermittlung geeignete technische Lösungen nach Absatz 2 unterliegen keiner Bewilligungspflicht.*
> *[4] Die Behörden, welche geeignete technische Lösungen nach Absatz 2 verwenden, sorgen für die dauerhafte Erfüllung der Eignungsvoraussetzungen nach Absatz 2. Sie dokumentieren dies und weisen es auf Verlangen nach.*

Erläuterungen:

- Absatz 1 stellt klar, dass für die Weitergabe bzw. Übermittlung elektronischer Akten zwischen Behörden des gleichen Kantons sowie zwischen Strafbehörden neben Plattformen nach dem BEKJ auch andere technische Lösungen eingesetzt werden können. Damit wird ausdrücklich berücksichtigt, dass in der behördlichen Praxis bereits heute sichere Schnittstellen und Fachapplikationen für den direkten elektronischen Aktenaustausch bestehen. Durch diese Formulierung werden die in den Spezialgesetzen unterschiedenen Fälle auf der Ebene der Ausführungsbestimmungen zusammengeführt.
- Absatz 2 definiert die Eignungsvoraussetzungen solcher technischen Lösungen. Entscheidend ist, dass die Zeitpunkte der Übermittlung eindeutig festgestellt werden können und dass die übermittelten Dokumente bzw. Dateien vor Veränderung sowie vor unberechtigter Kenntnisnahme geschützt sind. Diese Voraussetzungen sind bereits auf Gesetzesebene präzise genug festgelegt.
- Absatz 3 hält fest, dass in diesen Fällen auf eine Bewilligungspflicht verzichtet wird. Dadurch wird die Abgrenzung zu bewilligungspflichtigen Zustellplattformen geklärt und die bestehende Rechtsunsicherheit für andere Übermittlungslösungen beseitigt.
- Absatz 4 verpflichtet allerdings die nutzenden Behörden, die dauerhafte Einhaltung der Eignungsvoraussetzungen sicherzustellen, zu dokumentieren und auf Verlangen nachzuweisen. Damit wird gewährleistet, dass die nutzenden Behörden ihre Verantwortung für die Eignung der eingesetzten Lösung wahrnehmen.

Per E-Mail an

cornelia.perler@bj.admin.ch

Bern, 15. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ): Vernehmlassungsverfahren

Sehr geehrter Herr Bundesrat

Für die Gelegenheit zur Stellungnahme bedanken wir uns bestens.

Sie finden die Anmerkungen aus Sicht des Projektes Justitia 4.0 auf den folgenden Seiten.

Für die konstruktive Zusammenarbeit mit dem Bundesamt für Justiz bedanken wir uns und freuen uns auf den erfolgreichen Abschluss des Projekts. Gerne stehen wir bei Rückfragen zu Ihrer Verfügung.

Mit vorzüglicher Hochachtung

Yann-Eric Hofmann

Bundesrichter
Co-Präsident Steuerungsausschuss

Florian Düblin

Generalsekretär der KKJPD
Co-Präsident Steuerungsausschuss

Erläuterungen, Anregungen und Formulierungsvorschläge

Ingress

Im Vorentwurf fehlen bewusst die Artikel, die dem Bundesrat die Kompetenz zur Regelung des Formats der elektronisch übermittelten Dokumente übertragen. Im erläuternden Bericht wird präzisiert, dass, "um die Übersichtlichkeit zu bewahren", im Ingress lediglich die Bestimmungen der Verfahrensgesetze erwähnt werden, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben. Auch wenn ein allgemeiner Verweis auf das BEKJ angemessen erscheint, wäre es vorzuziehen, alle in den Verfahrensgesetzen enthaltenen Delegationsnormen zu erwähnen. Dies gilt insbesondere für die Artikel, die dem Bundesrat die Kompetenz zur Festlegung der Formate übertragen; diese sollten daher logischerweise ebenfalls im Ingress erwähnt werden.

Der Ingress sollte daher wie folgt ergänzt werden:

> *Der Schweizerische Bundesrat,*
> *gestützt auf das Bundesgesetz vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ),*
> *die Artikel 6a Absatz 2, 21a Absatz 2 und 34 Absatz 1bis des Verwaltungsverfahrensgesetzes vom 20.Dezember 1968 (VwVG),*
> *Artikel 38e des Bundesgerichtsgesetzes vom 17. Juni 2005 (BGG),*
> *die Artikel 128b Absatz 3, 128c Absatz 2 und 128e der Zivilprozessordnung (ZPO),*
> *die Artikel 33a Absatz 4, 33b, 33c Absatz 2 und 34 Absatz 3 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG),*
> *die Artikel 76a Absatz 2, 103b Absatz 3, 103c Absatz 2 und 103e der Strafprozessordnung (StPO),*
> *Artikel 2e des Bundesgesetzes vom 23. Dezember 2011 über den ausserprozessualen Zeugenschutz (ZeugSG),*
> *Artikel 31f des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht (VStrR),*
> *die Artikel 8c Absatz 3, 8d Absatz 2 und 8f des Opferhilfegesetzes vom 23. März 2007 (OHG)*
> *und die Artikel 37d und 38a Absatz 2 des Militärstrafprozesses vom 23. März 1979 (MStP),*
> *verordnet:*

1. Kapitel: Betrieb und Nutzung von Plattformen

1. Abschnitt: Geltungsbereich

Art. 1

Absatz 2 betrifft ausschliesslich bundesrechtliche Verfahren nach VwVG und ist **für kantonale Verwaltungsverfahren nicht relevant**.

Unklar scheint der Mehrwert von **Absatz 3**, gilt der Grundsatz der lex specialis doch ohnehin.

2. Abschnitt: Betriebsbewilligung

Art. 2 Anforderungen an die Plattformen

Die Anforderungen an die Plattformen scheinen sachgerecht. Aufgrund der schnellen technischen Entwicklung sollte die maximale Dateigrösse gemäss **Absatz 1 Buchstabe c** jedoch in einem Anhang zur vorliegenden Verordnung oder in einer Departementsverordnung des EJPD festgelegt werden.

Die **Löschfunktion in Absatz 1 Buchstabe d ist eine Funktionalität**, welche – wenn überhaupt - im 3. Abschnitt dieser Verordnung geregelt werden sollte. Zudem ist der Wortlaut der Bestimmung zu absolut formuliert und kaum umsetzbar. Wie der erläuternde Bericht auf Seite 11 zurecht ausführt, wird durch die Löschfunktion die erteilte individuelle Berechtigung gelöscht, nicht jedoch das Dokument als solches.

Bei einer Eingabe an oder einer Zustellung durch eine Justizbehörde haben sowohl der Absender als auch der Empfänger Zugriff auf das zugestellte Dokument. Wenn der Absender beispielsweise sein Zugriffsrecht löscht, verschwindet das Dokument aus der Ansicht seines Profils. Das Zugriffsrecht des Empfängers bleibt jedoch bestehen, sodass das Dokument weiterhin in seinem Profil sichtbar ist. Dies gilt für alle Beteiligten sowie für die jeweiligen Empfangs- und Abholquittungen. Das „Löschen" entspricht einer Verschiebung in den Papierkorb. Das effektive physische Löschen erfolgt gemäss den gesetzlichen Vorgaben (90 Tage) im Hintergrund.

Auf die Bezeichnung Benutzerkonto sollte im vorliegenden Zusammenhang verzichtet werden, da diese mehrere Profile enthalten können. Zudem enthalten die Profile aus technischer Sicht keine Dokumente oder Quittungen, sondern machen lediglich die bestehenden Zugriffsrechte sichtbar.

Absatz 1 Buchstabe d sollte daher wie folgt lauten:

> *d.* *Die Benutzerinnen und Benutzer können die Dokumente und Quittungen in der Ansicht ~~im Benutzerkonto~~ ihres Profils jederzeit ~~löschen~~ entfernen.*

Abs. 2

Die Weiterentwicklung der Schnittstellen ist ein laufender Prozess, entsprechend dynamisch entwickeln sich auch die Anforderungen. Das EJPD regelt die funktionalen und betrieblichen Anforderungen an die Schnittstellen. Das Projekt Justitia 4.0 lädt das EJPD beziehungsweise das BJ ein, im API-Forum mitwirken, wo die Weiterentwicklung der Schnittstellen mit den Nutzerinnen und Nutzern besprochen wird. Die Konsultation der Betreiberin, wie sie im erläuternden Bericht angesprochen wird, ist aus Sicht des Projekts Justitia 4.0 unerlässlich.

Art. 3 Bewilligungsverfahren

In der aktuellen Ausgangslage kann die Betriebsbetriebsbewilligung erst nach Inkrafttreten des BEKJ am 1. Juli 2027 erteilt werden. Allenfalls könnte die Bewilligung eine logische Sekunde nach Inkrafttreten des BEKJ und der Verordnungen erteilt werden. Das Bewilligungsverfahren sollte jedenfalls rechtzeitig eingeleitet werden, obwohl das Inkrafttreten der gesetzlichen Grundlage noch aussteht.

Besser wäre, wenn die Artikel 25, 27 und 28 des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz vorgängig in Kraft gesetzt werden, damit das Bewilligungsverfahren der zentralen Plattform rechtzeitig starten kann und die Betriebsbewilligung vor Inkrafttreten des ganzen Gesetzes auf dessen Inkrafttreten erteilt werden kann.

Jedenfalls wäre es wünschenswert, dass die Bewilligungsinstanz frühzeitig die Voraussetzungen bekanntgibt und das Bewilligungsverfahren soweit nötig koordiniert, vor allem wenn weitere Behörden oder Bundesämter in das Bewilligungsverfahren involviert sind, beispielsweise der EDÖB im Bereich Datenschutz oder die Fachstelle Betriebssicherheit des Staatssekretariats für Sicherheitspolitik SEPOS im Hinblick auf eine allfällige Betriebssicherheitsprüfung.

3. Abschnitt: Dokumente, Quittungen und Siegelung

Art. 4 Format der Dokumente

Der Vorentwurf verwendet – wie das BEKJ – den Begriff "Dokument" anstelle von Datei. In der Botschaft zum BEKJ (BBl 2023 679, S. 20) wird dies wie folgt begründet: "Der Begriff "Datei" ist für das Gesetz zu technisch."

In diesem Sinne ist in der Verordnung der Begriff Datei – an Stelle von Dokument – vorzuziehen, soweit es sich um technische Aspekte der übermittelten Aktenstücke handelt.

Abs. 1

Die Festlegung des Formats PDF/A für Dokumente von Behörden und der Formate PDF und PDF/A für die übrigen Verfahrensbeteiligten wird vom Projekt Justitia 4.0 begrüsst.

Abs. 2

In vielen Fällen kann der Informationsgehalt eines Dokuments im Format PDF rechtsgenüglich wiedergegeben werden. Insofern soll die Beilage in diesem weit verbreiteten Format eingereicht werden, was die Fallbearbeitung durch die Anwältinnen und Anwälte, die Staatsanwaltschaften, die Gerichte, die Verwaltungsbehörden und durch die weiteren Verfahrensbeteiligten erleichtert. Reichen die Verfahrensbeteiligte ihre Beilagen im Format PDF ein, entfällt die Konversion durch die Justizbehörden, allen Beteiligten liegt das gleiche Dokument vor. Die Digitalisierung soll die Verfahren beschleunigen und die Aktenführung vereinfachen. Wenn Dokumente im Regelfall als PDF-Dokument vorliegen, ermöglicht dies eine speditive Bearbeitung durch die Anwaltschaft und die Behörden. Geschäftsverwaltungssysteme der Anwältinnen, Anwälte und Behörden können aus Sicherheitsgründen nur mit einer beschränkten Anzahl an Dateitypen umgehen ('Whitelistening' von Fileformaten). Wenn das Format der Beilagen frei gewählt werden könnte, würde dies die Fallbearbeitung erheblich erschweren. Alle Verfahrensbeteiligten müssten zuerst nach dem passenden Programm suchen, um eine Datei zu öffnen. Zudem würde die uneingeschränkte Formatwahl ein erhebliches IT-Sicherheitsrisiko für alle Beteiligten darstellen.

In Einzelfällen kann das Format PDF den Informationsgehalt eines Dokuments nicht genügend wiedergeben. Zu denken ist beispielsweise an Audio- oder Videoaufnahmen, an mehrspurige Tunnelüberwachungen oder Aufzeichnungen aus Elektroautos. Für diese Fälle sollte das EJPD festlegen, welche Dateiformate direkt über die Plattformen übermittelt werden können. Aus Sicherheitsgründen scannt die zentrale Plattform alle Dateien auf Viren. Dabei kann die zentrale Plattform grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Für Dokumente, welche nicht direkt über die Plattformen übermittelt werden dürfen, besteht die Möglichkeit zur Übermittlung in einem Container, beispielsweise als Zip-Format.

Welche Dateiformate die Plattformen verarbeiten müssen, ist durch das EJPD nach Anhörung der Betreiberin der zentralen Plattform in einer Departementsverordnung zu regeln.

Absatz 2 sollte daher wie folgt lauten:

> [2] ~~*Die Beilagen können in jedem Format übermittelt werden.*~~ *Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage im Originalformat übermittelt werden.*

Abs. 3 und 4

Die vorgeschlagene Auswahl der Dateiformate wird begrüsst, kritisch wird dagegen die gewählte Normstufe beurteilt. Die Festlegung der Formate, welche verfahrensleitende Behörden bearbeiten müssen, sollte in einem Anhang zur VEKJ oder in einer Departementsverordnung des EJPD erfolgen.

Die Liste der unterstützten Dateiformate ist einem stetigen Wandel unterworfen. Es sind daher häufige Anpassungen zu erwarten. Zudem ist das reine Benennen von Formaten in der Verordnung nicht hinreichend. Es müssen weitere technische Details wie der Umgang mit passwortgeschützten oder verschlüsselten Dateien geregelt werden, gegebenenfalls bis hin zu einzelnen in einer offenen Datei dennoch verschlüsselten oder passwortgeschützten Elementen (z.B. Makros in einer Microsoft Excel-Datei, ZIP-Dateien mit teilweise verschlüsselten Dateien etc.). Dies ist in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung.

Absätze 3 und 4 sollten daher wie folgt lauten:

> [3] ~~*Die verfahrensleitende Behörde muss folgende Formate bearbeiten können:*~~
>
> ~~*a. schriftliche Unterlagen: PDF, PDF/A;*~~
>
> ~~*b. Bilddateien: BMP, GIF, JPEG, PNG;*~~
>
> ~~*c. Audiodateien: MP3, OGG, WAV;*~~
>
> ~~*d. Videodateien: AVI, MOV, MKV, MP4;*~~

~~*e. Archivdateien: ZIP, 7z.*~~

Kann die verfahrensleitende Behörde eine Beilage im Format, in dem sie eingereicht wurde, nicht öffnen, so räumt sie der einreichenden Partei eine angemessene Frist ein, damit diese die Beilage in einem von der Behörde festgelegten Format einreichen kann.

[4] ~~Wird eine Beilage in einem anderen Format eingereicht und kann die verfahrensleitende Behörde die Beilage nicht zweckmässig bearbeiten, so fordert sie die einreichende Person oder Behörde auf, die Beilage in einem von der verfahrensleitenden Behörde festgelegten Format einzureichen oder den Zugriff auf die Beilage in geeigneter Weise zu ermöglichen.~~ Das EJPD regelt die über die Plattformen zu übertragenden Dateiformate.

[5] ~~Sie räumt ihr eine angemessene Frist ein.~~

Art. 5 Quittungen

Die zentrale Plattform siegelt die Quittungen der Benutzerinnen und Benutzer, unabhängig davon, ob sie ein oder mehrere Dokumente übermitteln.

Die vorgeschlagene Regelung wird grundsätzlich begrüsst. Bei der elektronischen Kommunikation über die Plattform wird auf Unterschriften verzichtet. Behörden können dank ihrem individuellen Siegel identifiziert werden, welche sie vor der elektronischen Übermittlung auf ihren Dokumenten anbringen. Natürliche Personen werden über AGOV identifiziert. Organisationen dagegen verfügen über keine elektronischen Identifikatoren. Sie werden über die natürlichen Personen identifiziert, welche als Organ oder als Bevollmächtigte für die Organisation handeln. Entsprechend ist jedes Profil auf der zentralen Plattform, das nicht einer Behörde gehört, mit einer natürlichen Person als verantwortliche Person verknüpft.

Der Vorentwurf formuliert die Bestimmungen zu den Quittungen aus Sicht der Nutzerin oder des Nutzers ("Absenderin", "Adressat"). Das Projekt Justita 4.0 schlägt vor, diese Bestimmungen näher entlang der aktuellen technischen Ausgestaltung zu formulieren. Nach unserer Einschätzung resultiert daraus für die Nutzenden mehr Klarheit, da sich die in der Verordnung verwendeten Begriffe beispielsweise auch in der Eingabemaske der Plattform justitia.swiss wiederfinden.

Da die Behörde über ihr Siegel hinreichend identifiziert ist, soll der **Name der verantwortlichen Person des Profils einer Behörde** gemäss Absatz 2 Buchstabe b in der Quittung richtigerweise **nicht** aufgeführt werden. Nur der Name der Behörde soll auf der Quittung erscheinen.

Artikel 24 Absatz 4 des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz sieht vor, dass die Weitergabe von Berechtigungen aus den angebrachten elektronischen Siegeln nicht ersichtlich ist. Gleiches muss nach Ansicht des Projekts Justitia 4.0 auch für die Quittungen gelten. Die Weitergabe einer Berechtigung soll aus der Quittung nicht ersichtlich sein.

Auf der Quittung soll daher der Name des Profils, in dessen Namen der Versand erfolgt, und der Name der verantwortlichen Person aufgeführt sein (Absatz 2 Buchstabe b).

Absatz 2 Buchstabe d konkretisiert die Eingangsquittung und gibt unter anderem vor, dass die Angaben nicht übermittelter Dokumente auf der Eingangsquittung aufzulisten sind. Mögliche Gründe für eine Rückweisung durch die Plattform sind ein positives Resultat bei der Virenprüfung, die Dateigrösse oder ein Dateiformat, welches die Plattform nicht erkennt. Diese Bestimmung enthält einen logischen Fehler: Nicht übermittelte Dokumente können auf der **Eingangsquittung** nicht aufgeführt werden, da diese eben **nicht übermittelt** wurden. Die Quittung kann keine Hashwerte von Dateien enthalten, welche nicht übermittelt worden sind. Kann die Plattform ein oder mehrere Dokumente nicht übermitteln, so erhält die Absenderin oder der Absender eine Mitteilung der Plattform, jedoch keine Quittung. Absatz 2 ist daher wie folgt anzupassen:

[2] Die Quittungen müssen insbesondere folgende Angaben enthalten:

a. die Art der Quittung;

b. den Namen ~~der Absenderin oder des Absenders, ihre oder seine~~ des absendenden Profils, seine Adresse auf der Plattform und ~~gegenbenfall~~

~~c den Namen oder Die Firma der Organisation, für welche die Absenderin oder der Absender handelt~~ den Namen der verantwortlichen Person;

c. den Namen des adressierten Profils ~~oder die Firma der Adressatin oder des Adressaten~~ sowie ~~ihre oder~~ seine Adresse auf der Plattform;

d. bei einer Eingangsquittung:

1. die Liste der übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte,

~~2. die Liste der aufgrund des Resultats der Virenprüfung nicht übermittelten Dokumente und deren Grösse,~~

~~3.~~2. den Zeitpunkt der Übermittlung an die Plattform;

e. bei einer Abrufquittung: den Zeitpunkt des erstmaligen Abrufs;

f. bei einer Nichtabholquittung: den Zeitpunkt der Übermittlung an die Plattform;

g. beim Versand oder erstmaligen Abruf aufgrund der Weitergabe einer Berechtigung: den Namen ~~der Person~~ des Profils, in ~~deren~~ dessen Name der Versand oder Abruf erfolgt.

Die Plattformen müssen künftig auch strukturierte Daten übermitteln können, beispielsweise in Form von XML-Dateien. Die Ausnahmen in den Absätzen 4 und 5 sind daher wesentlich, da XML-Dateien aus technischen Gründen nicht gesiegelt werden können.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Im elektronischen Rechtsverkehr wird das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben. Die Plattform dagegen bringt ihr Siegel **nach** der Übermittlung auf die Plattform auf der ausgestellten Eingangsquittung gestützt auf Artikel 5 an.

Artikel 6 regelt die **Sieglung der Dokumente** durch die verfahrensleitende Behörde **vor der Übermittlung über eine Plattform** (Art. 22 Abs. 2 BEKJ). Der Vorentwurf führt aus, dass bei der Übermittlung von mehreren Dokumenten die Sieglung eines Dokuments genüge. Dies ist korrekt. Zu ergänzen ist, dass die Siegelung durch die verfahrensleitende Behörde unabhängig von der Anzahl der übermittelten Dokumente erfolgt. Auch ein einzelnes Dokument, welches die verfahrensleitende Behörde übermittelt, muss gesiegelt werden, damit die Authentizität des Dokuments unabhängig von einer Plattform überprüft werden kann.

Die Ausführungen im erläuternden Bericht, wonach eine Behörde alle Dokumente mit einem Siegel versehen muss, widersprechen dem Wortlaut der Verordnung: Die Siegelung eines Dokuments durch die verfahrensleitende Behörde genügt. Zudem entspricht die Siegelungspflicht für verfahrensleitende und verfahrensbeteiligte Behörden nicht dem technischen Konzept der zentralen Plattform.

Die **Unterscheidung zwischen verfahrensleitenden und verfahrensbeteiligten Behörden** ist für verschiedene Funktionalitäten essenziell, welche bei der zentralen Plattform bereits entwickelt und umgesetzt wurden. Beispielsweise können nur verfahrensleitende Behörden Zustellungen vornehmen. Nur die Adresse von verfahrensleitenden Behörden ist für Drittpersonen aus dem öffentlichen Verzeichnis der zentralen Plattform ersichtlich. Würde an der Siegelungspflicht für verfahrensleitende **und** verfahrensbeteiligte Behörden festgehalten, könnten alle Behörden uneingeschränkt und verfahrensunabhängig Zustellungen an andere Behörden, Organisationen und Privatpersonen vornehmen. Dies würde die zentrale Plattform für jegliche elektronische Kommunikation zwischen Behörden öffnen, wofür das BEKJ jedoch

keine hinreichende gesetzliche Grundlage bietet. Sinn und Zweck des BEKJ ist es, die elektronische Kommunikation in Justizverfahren zu ermöglichen.

Nur verfahrensleitende Behörden sind verpflichtet, ihre Dokumente elektronisch zu siegeln. Artikel 22 Absatz 2 BEKJ ist daher einschränkend auszulegen. Das elektronische Siegel stellt die Herkunft, den Zeitpunkt, die Integrität und die Authentizität des gesiegelten Dokuments sicher. Die Verfügung oder der Entscheid einer verfahrensleitenden Behörde begründen Rechte und Pflichten und entfalten Wirkung über das einzelne Verfahren hinaus. Betroffene müssen daher unabhängig von einem konkreten Verfahren oder von der zentralen Plattform prüfen können, ob das fragliche Dokument integer und authentisch ist und von der dafür zuständigen Behörde erstellt wurde. Das elektronische Siegel ist zusammengefasst genau dort notwendig, wo Behörden autoritativ auftreten.

Verfahrensbeteiligte Behörden dagegen dürfen nicht verpflichtet werden, ihre Dokumente zu siegeln. Die Dokumente, welche verfahrensbeteiligte Behörden in einem Justizverfahren übermitteln, begründen in der Regel keine neuen Rechte und Pflichten. Typischerweise handelt es sich bei diesen Dokumenten um Auszüge aus bestehenden Registern, Auszüge aus bestehenden Akten früherer Verfahren, bereits eröffnete Verfügung oder Entscheide aus abgeschlossenen Verfahren, welche nun für ein Justizverfahren zur Verfügung gestellt werden. Die Authentifizierung der verantwortlichen Person im Profil der Behörde auf der zentralen Plattform ermöglicht die korrekte Identifikation der Behörde. Will ein Verfahrensbeteiligter die Integrität oder Authentizität eines von einer verfahrensbeteiligten Behörde übermittelten Dokuments in Frage stellen, ist dies eine Frage der Beweiswürdigung im entsprechenden Verfahren.

Würde an der Siegelpflicht für alle Behörden gemäss erläuterndem Bericht festgehalten, so müssten alle Schweizer Behörden auf den Stufen Gemeinde, Kanton und Bund mit einem Siegel ausgestattet werden. Für die flächendeckende Ausstattung aller Schweizer Behörden mit einem elektronischen Siegel liefert das BEKJ keine genügende gesetzliche Grundlage. Für die Kantone und Gemeinden wäre die flächendeckende Einführung des elektronischen Siegels mit erheblichem organisatorischem Aufwand und beträchtlichen Kosten verbunden.

Gemäss erläuterndem Bericht müssen Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, nicht mehr gesiegelt werden. Diese Aussage entspricht nicht dem Konzept des BEKJ und der aktuellen Umsetzung durch die zentrale Plattform. Das BEKJ schreibt keine Funktionalität vor, wonach die zentrale Plattform qualifizierte elektronische Signaturen von Behördenmitgliedern einer Behörde zuordnet.

Da die Identifikation der Behörden mittels elektronischem Siegel erfolgt, verfügt die zentrale Plattform zur Zeit über keine Funktionalität, welche eine Prüfung von elektronischen Signaturen oder der Zuordnung von elektronischen Signaturen zu Behörden oder Organisationen ermöglicht. Daher müssen verfahrensleitende Behörden Dokumente, welche über eine qualifizierte elektronische Signatur verfügen, vor dem Versand über die Plattform standardmässig mit ihrem Siegel versehen.

Wichtig aus Sicht des Projekts Justitia 4.0 ist die Unterscheidung zwischen Zustellung und Akteneinsicht. Im Unterschied zur Zustellung besteht bei der Akteneinsicht, wie der erläuternde Bericht zu Artikel 7 ausführt, keine Pflicht zur Siegelung der Dokumente durch die verfahrensleitende Behörde.

Art. 7 Siegelung der Dokumente durch die Plattformen

Im elektronischen Rechtsverkehr soll das elektronische Siegel künftig an zwei verschiedenen Punkten eingesetzt werden. Die verfahrensleitende Behörde siegelt eines der übermittelten Dokumente **vor** der Übermittlung auf die Plattform, in der Regel wohl die Verfügung, den Entscheid oder das Begleitschreiben (Art. 6). Artikel 7 bezieht sich dagegen auf die Siegelung der Quittung **nach** der Übermittlung durch die zentrale Plattform.

Abs. 1

Dieser Grundsatz stützt sich auf Artikel 2 Buchstabe a des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES). Demnach handelt es sich bei einer elektronischen Signatur um Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen. Der Grundsatz der Siegelung durch die Plattformen wird im Vorentwurf korrekt wiedergegeben: Träger

des Siegels der Plattform ist die **Quittung, nie das übermittelte Dokument oder die übermittelte Datei.** Im Falle der zentralen Plattform handelt es sich dabei um die sogenannte Eingangs- oder Abrufquittung. Die zentrale Plattform siegelt die Quittungen der Benutzerinnen und Benutzer, unabhängig davon, ob sie ein oder mehrere Dokumente übermitteln. Absatz 1 sollte daher wie folgt lauten:

> [1] *Werden ~~mehrere~~ Dokumente ~~zusammen~~ übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an. Das Dokument muss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.*

Abs. 2

Absatz 1 beschreibt die Siegelung der Quittungen durch die zentrale Plattform korrekt. Die Übermittlung von gesiegelten Dokumenten folgt den gleichen Regeln wie in Absatz 1. **Absatz 2 muss daher gestrichen werden**.

> ~~[2] *Dokumente, die bereits über ein Siegel oder eine qualifizierte elektronische Signatur mit einem Zeitstempel verfügen, müssen nicht erneut mit einem Siegel versehen werden.*~~

4. Abschnitt: Authentifizierung, Profile, Schnittstellen und Berechtigungen

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Die Authentifizierung über AGOV gemäss Absatz 1 ist sinnvoll und zielführend. Die detaillierten Anforderungen sollten in einer Departementsverordnung des EJPD geregelt werden.

Der mögliche Einsatz von zusätzlichen Authentifizierungsdiensten bei künftigen kantonalen Plattformen gemäss Absatz 2 wird begrüsst.

Künftig sind die meisten Behörden über eine Schnittstelle mit der zentralen Plattform verbunden. Absatz 3 lässt genügend Spielraum, um künftige technische Lösungen umzusetzen.

Art. 9 Profile

Gemäss aktueller Umsetzung der Plattform ist jedem (nicht Behörden-)Profil eine natürliche Person mit eigenem Benutzerkonto als verantwortliche Person zugewiesen. Der Name der verantwortlichen Person erscheint im Adressverzeichnis der zentralen Plattform, das für Behörden sichtbar ist, und auf den ausgestellten Quittungen. Im öffentlichen Adressverzeichnis sind dagegen nur die Adressen der verfahrensleitenden Behörden ersichtlich.

Der Name der verantwortlichen Person ermöglicht die Identifikation der Organisation, in deren Namen die verantwortliche Person handelt. Die verantwortliche Person kann weitere Mitglieder, die über ein eigenes Benutzerkonto verfügen, dem von ihr verantworteten Profil hinzufügen. Der Name der weiteren Mitglieder ist weder im Verzeichnis noch aus den Quittungen ersichtlich. Die verantwortliche Person wird regelmässig aufgefordert, die Berechtigung der eingeladenen Mitglieder zu überprüfen. Die verantwortliche Person kann ihre Rolle an eine andere Benutzerin, einen anderen Benutzer übertragen.

Bei einem Behördenprofil erscheint der Name der verantwortlichen Person weder im Adressverzeichnis noch auf der Quittung.

Abs. 1

Der Absatz 1 ist sehr absolut formuliert und berücksichtigt zu wenig die Besonderheiten des Behördenprofils. Es könnte auch missverstanden werden, so dass aufgrund der Systematik (Absatz 1) der Eindruck entsteht, dass jeder Benutzer ohne weiteres ein Behördenprofil anlegen könnte. Es wird angeregt, Absatz 1 neu an den Schluss von Artikel 9 zu verschieben.

Für die übrigen Benutzerinnen und Benutzer entspricht Absatz 1 der aktuellen Umsetzung durch die zentrale Plattform, wonach jede Benutzerin und jeder Benutzer mehrere Profile anlegen kann. Im Umkehrschluss basiert jedes (nicht Behörden-)Profil auf dem Benutzerkonto einer natürlichen Person.

Abs. 2

Diese Bestimmung bezieht sich einzig auf verfahrensleitende Behörden, die über ein elektronisches Siegel verfügen und im (öffentlichen) Adressverzeichnis der zentralen Plattform erscheinen. Bei verfahrensleitenden Behörden ist auf die Angabe einer postalischen Adresse zu verzichten, da die Suche nach der Plattformadresse einer Behörde nach Einschätzung des Projekts Justitia 4.0 nicht über das Adressverzeichnis der Plattform, sondern über die Webseite der jeweiligen Behörde erfolgt. Bei Bedarf kann in die Bezeichnung der Behörde ein Zusatz oder der Standort aufgenommen werden. Im Verzeichnis der aktuell anerkannten Zustellplattformen (Inca-Mail und PrivaSphere) sind weder Privat- noch Geschäftsadressen aufgeführt. Die Bestimmung in Absatz 2 ist entsprechend anzupassen.

> [2] *Die Profile von Behörden müssen mindestens folgende Angaben enthalten:*
>
> *a. Name der Behörde;*
>
> *~~b. Postadresse;~~*
>
> *~~c~~ b. Bezeichnung ihres Siegels.*

Abs. 3

Die Übernahme des Geburtsdatums aus dem AGOV-Account wurde in der zentralen Plattform bereits konzipiert. Gemäss aktueller Umsetzung dient das Geburtsdatum der Identifikation einer natürlichen Person. Die Suche nach Benutzerinnen und Benutzer mit einem bestimmten Geburtsdatum ist dagegen technisch nicht möglich.

Zu betonen ist, dass die Privatadresse im AGOV-Account nicht automatisch aktualisiert wird. Die Privatadresse beruht auf der Selbstdeklaration der Nutzerin oder des Nutzers. Sie wird anlässlich der Identifikation nicht geprüft, weshalb sie nicht verlässlich ist. Auch aus Sicht des Datenschutzes ist die Speicherung der Privatadresse in den Benutzerprofilen als kritisch zu betrachten. In den Profilen der natürlichen Personen sollte daher auf die Erhebung von Postadressen **verzichtet werden**.

Organisationen haben unterschiedliche Strukturen und gegebenenfalls verschiedene Niederlassungen, weshalb das verwendete digitale Profil nicht mit der offiziellen Postadresse übereinstimmen muss. Die Postadresse bringt bei der digitalen Zustellung keinen nennenswerten Mehrwert. **Bei Organisationen soll daher auf die Postadresse verzichtet werden.**

Während verfahrensleitende Behörden über ihr Siegel identifiziert werden, erfolgt die Identifikation von Organisationen über die verantwortliche Person, welche dem Profil der Organisation zwingend zugeordnet ist. Der Name der verantwortlichen Person soll daher im Profil und im Verzeichnis der Plattform ersichtlich sein.

Absatz 3 sollte daher wie folgt lauten:

> *[3] Die Profile der übrigen Benutzerinnen und Benutzer müssen mindestens folgende Angaben enthalten:*
>
> *a. bei natürlichen Personen: Vorname, Name und Geburtsdatum ~~sowie Postadresse~~;*
>
> *b. bei Organisationen: Name oder Firma und ~~Postadresse~~ Name der verantwortlichen Person.*

Abs. 4

Nach Einschätzung von Justitia 4.0 Absatz 4 betrifft Absatz 4 die Kommunikation zwischen professionellen Vertreterinnen und Vertretern und der verfahrensleitenden Behörde. Gemäss Wortlaut sind von der Bestimmung nur Anwältinnen und Anwälte erfasst, die für eine Organisation tätig sind. Unklar ist, ob Parteivertreter, die alleine oder in Bürogemeinschaft tätig sind, ebenfalls einen Zusatz führen müssen, um als Parteivertreter erkennbar zu sein. Durch die Einführung der verantwortlichen Person ist aus dem Profil

und der entsprechenden Quittung ersichtlich, welche Rechtsanwältin, welcher Rechtsanwalt handelt. Daher kann auf Absatz 4 verzichtet werden.

Besser wäre ein optionales Feld mit einer Zusatzangabe als Freitext, Bsp.: *Rechtsanwältin* oder *Kanzlei Hirschengraben*. Diese Lösung ist möglich, da in Absatz 3 nur die Mindestangaben festgelegt werden.

Art. 10 Schnittstelle

Dieser Artikel erlaubt den Nutzenden der Plattformen, ihre Systeme via eine Schnittstelle mit der Plattform zu verbinden und ihre Mitarbeitenden mit Vertretungsrechten auszustatten. Dies geschieht über einen technischen Benutzer, der ein digitales Passwort (Token) erhält. Die vorgeschlagene Regelung wird vom Projekt Justitia 4.0 begrüsst.

Art. 11 Bestätigung und Entzug der Berechtigungen

Die vorgeschlagene Regelung in Absatz 1 wird begrüsst. Jedoch sollte in der französischen Version wohl eher von *Confirmation* als von *Attribution* gesprochen werden.

Die vorgeschlagenen Variante in Absatz 2 wird begrüsst.

5. Abschnitt: Datenschutz, Datensicherheit und Virenprüfung

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Artikel 12 sieht vor, Dokumente und Quittungen nach Ablauf der Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten. Die automatisierte Löschung von Dokumenten und Quittungen nach einer überschaubaren Zeitspanne ist zu begrüssen, zumal die Plattform ein «Briefkasten» und keine Langzeitablage sein soll. Aus Gründen der Einheitlichkeit und der Datensparsamkeit begrüsst das Projekt Justitia 4.0 die vorgeschlagene Lösung.

Art. 13 Datensicherheit

Die vorgeschlagene Bestimmung verweist auf den 3. Abschnitt, die Angabe des relevanten Kapitels (2.?) fehlt und sollte ergänzt werden, zudem ist der einleitende Verweis auf die Verordnungsbestimmung unvollständig.

Artikel 13 sollte daher wie folgt lauten:

> *Die Datensicherheit der von den Kantonen zur Verfügung gestellten Plattformen nach Artikel 1 Absatz 1 Buchstabe b richtet sich nach dem 3. Abschnitt X. Kapitel des Informationssicherheitsgesetzes vom 18. Dezember 2020 und Artikel 8 des Datenschutzgesetzes vom 25. September 2020.*

Art. 14 Virenprüfung

Bei der vorgesehenen Prüfung auf Schadsoftware sind aus technischer Sicht drei Fälle zu unterscheiden:

1. Vollständige Prüfung der übermittelten Dateien: Die Maximalgrösse der einzelnen Dateien darf eine festgelegte Obergrenze nicht überschreiten, da die Prüfsoftware sonst ihr Limit (Speicherplatz usw.) erreichen, die Prüfung abbrechen und der Prüfvorgang so viel Zeit in Anspruch nehmen könnte, dass die Einhaltung von Fristen, besonders bei einer zeitlich knappen Eingabe, gefährdet wäre.

2. Eingeschränkte Prüfung grosser Dateien: Eine Datei, welche die festgelegte Obergrenze überschreitet, wird zum Zweck der Schadsoftware-Prüfung in handhabbare Blöcke zerlegt, die dann einzeln auf Schadsoftware geprüft werden. Dieses Verfahren ist jedoch weniger zuverlässig als die vollständige Prüfung der übermittelten Dateien. Schadsoftware, die durch die Aufteilung in prüfbare Blöcke auf zwei aufeinanderfolgende Blöcke verteilt wird, wird unter Umständen nicht mehr als Schadsoftware erkannt. Dies muss den Nutzerinnen und Nutzern der Plattform verständlich angezeigt werden. Insbesondere ist dem Empfänger klar zu signalisieren, dass er **eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten nach dem Herunterladen der Datei vornehmen muss.**

3. Keine Virenprüfung: Die zentrale Plattform kann die Virenprüfung nicht durchführen oder sie verzichtet auf Ersuchen der Benutzerin oder des Benutzers darauf.

Während der Pilotierung der zentralen Plattform hat sich gezeigt, dass die ergriffenen Schutzmassnahmen unter Umständen zu strikt sind und Dokumente aus verschiedenen Gründen zurückgewiesen wurden. Folgende Ursachen wurden während der Pilotierung identifiziert (nicht abschliessend):

- Übermittlung von passwortgeschützten oder end-2-end verschlüsselten Dateien zwischen bestimmten Behörden. Diese Dateien können prinzipiell nicht auf Schadsoftware geprüft werden, da sie verschlüsselt sind.
- Übermittlung von Dateiformaten mit Makros oder anderem ausführbaren Code: Diese enthalten zwar keine Viren im klassischen Sinne, bieten jedoch zahlreiche Angriffsmöglichkeiten für Cyberkriminelle. Aus diesem Grund werden ausführbare Dateiformate durch die Pilotplattform abgewiesen.
- Übermittlung von elektronischen Beweismitteln aus beschlagnahmten Geräten, im Original oder nach Aufbereitung durch die IT-Forensik, zum Beispiel im Rahmen der Akteneinsicht.
- Durch die ergriffenen Schutzmassnahmen werden Dateien fälschlicherweise zurückgewiesen, obwohl die Dateien von den sendenden Behörden bereinigt worden sind (sogenannte False-Positive).

In der Pilotierung wurde mehrfach gefordert, dass auch kritische Dateien übermittelt werden können, beispielsweise in einem digitalen Container. Die Behörden sollen dafür nicht auf alternative, unsichere Übermittlungswege ausweichen müssen (E-Mail, Cloud, UBS-Sticks, etc.). Die Ablage und Abholung dieser Dateien und die Prüfungen auf Schadsoftware obliegen in diesen Fällen den Nutzerinnen und Nutzern der Plattform. Wollen Sender und Empfänger auf Schutzmassnahmen verzichten, reduzieren sie die Funktion der Plattform auf die reine Übermittlung von Daten und sind selbst für den korrekten Umgang mit den Dateien verantwortlich. Dies bedingt eine ausdrückliche Absprache zwischen den Beteiligten. **Dies bedeutet auch, dass Nutzerinnen und Nutzer eine eigene, vollständige Schadsoftware-Prüfung auf den lokal gespeicherten Daten jeweils vor und nach Übermittlung durch die zentrale Plattform vornehmen müssen.** Die Plattform muss den Empfänger zudem darauf hinweisen, dass die in einem Container übermittelten Dateien keiner Virenprüfung unterzogen worden sind. Zudem obliegt es der Nutzerin oder dem Nutzer, die zu übermittelnden Dateien in ein von der Plattform akzeptiertes Containerformat zu packen. Die Plattform bietet diese Funktionalität gemäss aktuellem Stand nicht an.

Abs. 1

Die Festlegung der (Maximal-)Grösse von prüfbaren Blöcken grösserer Dateien sollte nicht öffentlich kommuniziert werden. Diese Information ist für die Nutzerinnen und Nutzer der Plattform irrelevant. Sie eröffnet potenziellen Angreifern jedoch die Möglichkeit, ihre Schadsoftware in einer verseuchten Datei so anzuordnen, dass der Schadcode bei der Aufspaltung in mehrere Blöcke in zwei aufeinanderfolgenden Blöcken liegt und nicht zuverlässig als schädlich erkannt werden kann. Zudem wird es stark von der für die Aufspaltung und Prüfung zuständigen Software abhängen, wie gross diese prüfbaren Blöcke zu gestalten sind. Diese Grenze wird sich aufgrund von Betriebserfahrung und Verbesserungen in der Hard- und Software dynamisch verändern und sollte einfach anpassbar sein.

Absatz 1 sollte zusammengefasst wie folgt lauten:

> [1] *Die Plattformen ~~müssen bei bis zu 64 Megabyte grossen Dateien~~ führen eine Virenprüfung durch~~führen~~.*

Abs. 2

Der Grenzwert für eine vollständige Prüfung auf Schadsoftware von derzeit 64 MB kann (und sollte) basierend auf den technischen Möglichkeiten und der wachsenden Betriebserfahrung durch die Betreiber der Plattformen erhöht werden können. **Absatz 2 ist daher zu streichen**.

[2] ~~Dokumente ab 64 Megabyte können sie in 64 Megabyte grosse Dokumente aufteilen und diese einer Virenprüfung unterziehen.~~

Abs. 3

Der Verzicht auf die Virenprüfung steht in einem engen Zusammenhang mit den zulässigen Formaten der Dokumente (Art. 4). Dokumente, welche die zentrale Plattform aufgrund ihres Formats nicht übermitteln kann oder welche in der Virenprüfung fälschlicherweise als positiv erkannt wurden, können in einem Container übermittelt werden, vorausgesetzt Absender und Empfänger stimmen der Übermittlung zu.

Abs. 4

Eine klare Kennzeichnung ist auch dann essenziell, wenn die Virenprüfung nur eingeschränkt stattgefunden hat. Absatz 4 ist dementsprechend zu ergänzen. Unklar ist allerdings, wie die Ergebnisse der Virenprüfung den Nutzenden mitgeteilt werden. Die Mitteilung sollte technisch einfach und inhaltlich leicht verständlich erfolgen können.

Absatz 4 sollte wie folgt lauten:

[4] Dokumente, bei denen ~~eine Virenprüfung nach Absatz 2~~ keine oder eine eingeschränkte Virenprüfung durchgeführt wurde, müssen entsprechend gekennzeichnet werden.

Abs. 5

Bei der Information der Plattformen an die Absenderin oder den Absender, dass ein Dokument nicht übermittelt werden konnte, handelt es sich klarerweise nicht um eine Quittung, da eben kein Dokument übermittelt worden ist (vgl. Ausführungen zu Art. 5 Abs. 2 Bst. d Ziff. 2 oben).

Für die Anwältinnen und Anwälte ist es wichtig, dass die Ablehnung von Dokumenten durch die Plattform hinreichend dokumentiert ist. Im Moment erarbeitet das Team von Justitia 4.0 eine erste Lösung, bei welcher die Nutzerin oder der Nutzer die Anzeige der Fehlermeldung bei der Nichtübermittlung eines Dokuments speichert.

6. Abschnitt: Gebühr für die Nutzung der zentralen Plattform

Basis für die Berechnung der Gebühr bilden die Artikel 6 und 32 des BEKJ. Die Kosten der zentralen Plattform werden auf die nutzenden Kantone aufgeteilt. Für die Mitglieder der Körperschaft berechnet sich der Gebührenanteil anhand der ständigen Wohnbevölkerung. Mit Nichtmitgliedern schliesst die Körperschaft eine Vereinbarung gemäss Artikel 6 BEKJ ab. Die vereinbarte Vergütung soll sämtliche Kosten decken (inklusive Investitionskosten, Botschaft BEKJ, BBl 2023 679, S. 22), welche das Nichtmitglied verursacht. Die Kosten für Nichtmitglieder werden daher in der Regel höher ausfallen als jene der Mitglieder.

Art. 15 Berechnung der Gebühr

Die deutsche und die französische Fassung wurden verglichen und vereinheitlicht; dies betrifft auch die konsistente Terminologie für denselben Sachverhalt. Für mehr Klarheit wurde der Absatz 1 in (neu) zwei Absätze aufgeteilt.

Die Dreijahresfinanzplanung als Referenz für die Festlegung des Gesamtbetrags für drei Jahre wird begrüsst. Der Ansatz liefert eine vorausschauende und realistische Grundlage für die jährlich gemäss Verteilschlüssel in Artikel 16 festzulegende Gebühr. Das ergänzende Korrektiv gemäss Absatz 4 stellt die notwendige Anpassungsfähigkeit sicher.

Folgender Text wird vorgeschlagen:

[1] ~~Die Gesamthöhe~~ Der Gesamtbetrag der jährlich von den Mitgliedern der öffentlich-rechtlichen Körperschaft zu entrichtenden Gebühr ~~für die Nutzung der zentralen Plattform~~ muss die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform decken und die Bildung einer Reserve für die Sicherstellung der Liquidität der öffentlich-rechtlichen Körperschaft in der Höhe von 10 Prozent der jährlichen Betriebskosten ~~ermöglichen~~ gewährleisten.

[Anpassung und neuer Absatz 2]

[2] ~~Die Einnahmen aus Leistungsbezügen der~~ Beiträge von Kantonen, die nicht Mitglied der öffentlich-rechtlichen Körperschaft sind, werden vom Gesamtbetrag der jährlichen Gebühr abgezogen.

[3] Das EJPD legt ~~die jährliche~~ den Gesamtbetrag der jährlichen Gebühr ~~aufgrund~~ für jeweils drei Jahre im Voraus auf der Grundlage der Finanzplanung der öffentlich-rechtlichen Körperschaft fest.

[4] Das EJPD kann die Gebühr während der Periode nach Absatz 3 ~~2~~ anpassen, wenn die eingenommenen Beiträge nach Absatz 1 und 2 ~~diese Gebühr~~ die Betriebs- und Weiterentwicklungskosten nicht ~~deckt~~ decken oder die Reserve die Limite nach Absatz 1 überschreitet.

Art. 16 Aufteilung der Gebühr

Die Bundesverwaltung nutzt die Plattform gemäss aktuellem Planungsstand für Verwaltungsstrafverfahren des Bundes, nicht aber für die erstinstanzlichen Verwaltungsverfahren. Der Bundesanteil von 10 Prozent wird daher begrüsst. Nach der vollständigen Einführung des Obligatoriums ist zu prüfen, ob die effektive Nutzung dem vorgeschlagenen Gebührenmodell entspricht oder ob eine Anpassung der Gebührenverteilung vorgenommen werden muss, insbesondere mit Blick auf die Anzahl der verwaltungsstrafrechtlichen Übermittlungen. Eine Überprüfung der Berechnungsweise der Gebühr ist denn auch in Artikel 21 vorgesehen. Auch die Aufteilung der Gebühr sollte Gegenstand der Prüfung sein.

Die Aufteilung gemäss ständiger Wohnbevölkerung in Absatz 2 wird begrüsst. Grundlage können jedoch nur statistische Daten sein, welche im Zeitpunkt der Berechnung vorliegen. Anhand dieser verbindlichen Angaben legt das EJPD den jährlichen Gebührenbeitrag fest; es berücksichtig dabei die in Artikel 15 Absatz 4 definierten Schwellenwerte und den allfälligen Beitritt eines Nichtmitgliedes zur Körperschaft justitia.swiss nach deren Gründung (vgl. Art. 19 Vereinbarung justitia.swiss sowie erläuternder Bericht zur Vereinbarung justitia.swiss, S. 17).

Vorgeschlagen wird folgender Wortlaut:

[1] Die Gesamthöhe der Gebühr wird wie folgt auf den Bund und die Kantone, die Mitglied der öffentlich-rechtlichen Körperschaft sind, aufgeteilt:

a. Bundesverwaltung und Bundesanwaltschaft (BA): 5 Prozent;

b. Eidgenössische Gerichte: 5 Prozent;

c. Kantone: 90 Prozent.

[2] Der Anteil der Kantone wird ~~gemäss der im Zeitpunkt der Festlegung der Gebühr ständigen Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt~~ unter den Kantonen, die Mitglieder der öffentlich-rechtlichen Körperschaft sind, proportional zu deren ständigen Wohnbevölkerung am 1. Januar des Vorvorjahres, für das die Gebühr fällig wird, verteilt; massgeblich ist die Anzahl Einwohnerinnen und Einwohner nach dem Bundesstatistikgesetz vom 9. Oktober 1992, dem Volkszählungsgesetz vom 22. Juni 2007 und den dazugehörigen Verordnungen ~~im Zeitpunkt der Festlegung nach Artikel 15~~.

[3] Das EJPD legt jährlich die Verteilung der Gebühr auf die Kantone fest.

Art. 17 Gebührenanteil der Bundesverwaltung und der Bundesanwaltschaft

Keine Bemerkungen.

Art. 18 Gebührenanteil der eidgenössischen Gerichte

Keine Bemerkungen.

Art. 19 Fälligkeit

Die Verordnung lässt die weiteren Modalitäten der Erfüllung offen. Es ist anzunehmen, dass die Regeln des Obligationenrechts sinngemäss zur Anwendung kommen. Vorgeschlagen wird daher folgender Wortlaut der Bestimmung:

> [1] *Die jährliche Gebühr der Mitglieder der öffentlich-rechtlichen Körperschaft ist ~~sind~~ im Voraus zu entrichten und am 1. Januar fällig.*
>
> [2] *Die Gebühr für ~~das erste Betriebsjahr der öffentlich-rechtlichen Körperschaft ist an dem Tag fällig, an dem diese Verordnung in Kraft tritt~~ die Nutzung der zentralen Plattform ist erstmals am Tag des Inkrafttretens dieser Verordnung fällig.*
>
> [3] *Die Bestimmungen des Obligationenrechts zum Schuldnerverzug finden sinngemäss Anwendung.*

Art. 20 Rechnungsstelle der Kantone

Keine Bemerkungen.

Art. 21 Evaluation der Gebührenregelung

Die Überprüfung der Berechnungsweise und der Aufteilung der Gebühr wird begrüsst.

2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten

Art. 22 Digitalisierung von physischen Dokumenten

Grundsätzlich wird diese Bestimmung begrüsst.

Das in Absatz 2 vorgeschriebene Format PDF/A erleichtert die Archivierung der Justizakten. Unklar ist, ob dieses Format durch die sehr unterschiedlichen kantonalen Justizapplikationen leicht verarbeitet werden kann.

Absatz 3 sieht die Texterkennung vor. Diese scheint in vielen Fällen sinnvoll und erleichtert die Bearbeitung der Dokumente. Bei fremdsprachigen Texten kann das Ergebnis der Texterkennung gemäss aktuellem Stand der Technik jedoch unbefriedigend oder fehlerhaft sein. Die Auflösung (DPI) sollte nach Einschätzung von Justitia 4.0 in der Verordnung nicht fest vorgegeben werden. Die optimale DPI-Zahl hängt stark vom jeweiligen Originaldokument ab. Für normale Textdokumente sind in der Regel 150 DPI ausreichend, während es bei Bildern sinnvoll sein kann, mit einer höheren Auflösung zu scannen.

Art. 22*a* (neu) Rücksendung von physischen Dokumenten

Problemstellung

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7) wird dargelegt, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Artikel 30 BEKJ in die vorliegende Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe.

Diese Feststellung bezieht sich auf die Auslegung des in Artikel 30 BEKJ enthaltenen Begriffs der «Dokumente», der im Gesetz weder nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird. Eine differenzierende Betrachtung ist nach hier vertretener Auffassung jedoch erforderlich, um mit einer lückenhaften Verordnung zum BEKJ neue Probleme zu schaffen, die es in der analogen Welt noch nicht gibt. Damit ist auch gesagt, dass die anwendbaren Prozessgesetze nach hier vertretener Meinung durchaus Raum für eine Auslegung der Bestimmungen des BEKJ im Sinne ihrer gesetzgeberischen Zielsetzung lassen.

Insbesondere im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch

nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen in Papierform eingehen, weil derlei Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der zentralen Plattform registrieren wollen. Diese riesige Menge an Eingaben wird speziell für die Strafbehörden geschrieben und oftmals mit Fotokopien rechtserheblicher Dokumente ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die es in der analogen Welt bisher nicht gab. Dies kann nicht der Wille des Gesetzgebers gewesen sein.

Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft, die im Schriftstück enthalten ist. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden überwiegend weggeworfen werden, sobald sie wieder bei ihren ursprünglichen Absenderinnen und Absendern eingetroffen sind.

Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, könnte mit den zurückgeschickten Dokumenten nicht Beweis geführt werden, weil sich nicht feststellen liesse, ob es auch diese Papiere waren, die gegenüber der Behörde eingereicht worden waren.

Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Artikel 30 Absatz 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Der Botschaft zum BEKJ ist zu entnehmen, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen (Botschaft BEKJ, BBl 2023 679, S. 36). Damit ist auch gesagt, dass die Rücksendepflicht von Urkunden, an deren Wiedererhalt die Absenderinnen und Absender ein Interesse haben, vorliegend nicht in Frage gestellt wird.

Hingegen braucht nicht weiter ausgeführt werden, dass durch die Auslegung des BEKJ im Sinne eines neu geschaffenen, replizierenden Postverkehrs in Papierform ein enormer Mehraufwand durch Porti und Arbeitsaufwand geschaffen wird. Eine Gesetzesauslegung, die letztlich dazu führt, dass tausende von Altpapierbündeln mit Porto versehen werden müssen, kann nicht von der gesetzgeberischen Absicht getragen sein.

Lösungsansatz

Aus den oben genannten Gründen wird vorliegend vorgeschlagen, einen neuen Artikel 22a einzufügen. Die gewählte Formulierung stellt klar, dass Dokumente, die gemäss Artikel 30 Absatz 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Wenn hingegen eines der danach genannten Kriterien zutrifft, ist sichergestellt, dass die Absenderin oder der Absender keinerlei Mehrwert von einer Rücksendung hat, weshalb es notwendig scheint, unter Rückgriff auf den gesetzgeberischen Normzweck eine Negativauslegung des Dokumentenbegriffs gemäss Artikel 30 BEKJ in die Verordnung zu schreiben. Sollte die Absenderin oder der Absender ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen:

> *2. Kapitel: Digitalisierung und Rücksendung von physischen Dokumenten sowie Papierversand von elektronisch erstellten Dokumenten*
>
> […]
>
> *Art. 22a Rücksendung von physischen Dokumenten*
>
> *Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn*

ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.

Art. 22*b* (neu) Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten

Problemstellung: Wie erreicht man Personen, welche nicht auf der Plattform erreichbar sind?

In Ziffer 2.6 des erläuternden Berichts zur Eröffnung des Vernehmlassungsverfahrens (S. 7 f.) wird ausgeführt, die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, sei verworfen worden, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Artikel 353 Absatz 1 Buchstabe k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: «Der Strafbefehl enthält: (…) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.» Artikel 238 Buchstabe h nZPO enthält eine ähnliche Regelung für zivilgerichtliche Entscheide.

Artikel 22 konkretisiert Artikel 29 BEKJ (Digitalisierung physischer Dokumente) und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück. Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ zwar die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird.

Insbesondere Übertretungsstrafbehörden und die Strafbefehlsabteilungen der Staatsanwaltschaften erlassen jedes Jahr zehntausende von Endentscheiden. Werden diese Verfahren aus der elektronischen Aktenführung ausgeklammert, weil sie gemäss der (nunmehr unterbliebenen) Auslegung der massgebenden Verfahrensbestimmungen durch die Verordnung zum BEKJ doch wieder in Papierform geführt werden müssten, verbleibt noch eine Menge von zehn bis zwanzig Prozent der Dossiers, die überhaupt elektronisch geführt werden können. Insbesondere im Bereich des Massengeschäfts verpufft damit das Rationalisierungspotential der Digitalisierung.

Zwar liegt dem BEKJ als Regulierungsgrundsatz die Idee zugrunde, dass Privatpersonen nicht zur elektronischen Kommunikation mit den Behörden gezwungen werden sollen und an dieser Grundlage soll vorliegend deshalb auch nicht gerüttelt werden. Hingegen kann es nicht richtig sein, das Unterschriftserfordernis derart restriktiv auszulegen, dass jeglichem Fortschritt ein Riegel vorgeschoben wird.

Artikel 22 Absatz 2 BEKJ ist zu entnehmen, dass künftig mittels eines geregelten elektronischen Siegels sichergestellt werden soll, dass ein elektronisch erstelltes Dokument tatsächlich von der zuständigen Behörde stammt, die sich etwa aus dem Briefkopf o.ä. ergibt. Zu diesem Artikel ist der Botschaft zum BEKJ zu entnehmen: «Das Unterschriftserfordernis stellt bei der Digitalisierung oft ein Hindernis dar. Anstelle der Unterschrift sieht das Gesetz die Authentifizierung mit Hilfe eines anerkannten elektronischen Identitätsnachweises sowie dem Anbringen eines geregelten elektronischen Siegels vor.» (Botschaft BEKJ, BBl 2023 679 S. 30). Damit ist gesagt, dass das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift ersetzt. Für einen Rückgriff auf Artikel 14 OR bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel (zum Schutzniveau vgl. Botschaft BEKJ, a.a.O.).

Lösungsansatz

Zwar ist dem erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens insoweit beizupflichten, dass den massgeblichen Verfahrensgesetzen zu entnehmen ist, dass etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Nach hier vertretener Auffassung lässt diese Formulierung aber durchaus eine Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes zu.

Bereits heute ist es absolut gängige Praxis bei den Zivilgerichten und den Strafbehörden, das Original der Endentscheide zu den Akten der Behörde zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen. Wie schon weiter oben zur Bestimmung über den Rückversand eingesandter Papierdokumente ausgeführt, wird nun durch den Verzicht auf eine reduzierende Auslegung eine neue Pflicht in der analogen Welt geschaffen. Wird dem erläuternden Bericht gefolgt, soll es plötzlich eine Pflicht zum Versand von Papieroriginalen geben. Damit wird der Versand von Papieroriginalen in der digitalen Welt exponentiell vervielfacht. Das kann nicht die Idee der Gesetzgebung gewesen sein.

Entsprechend ist in der Verordnung klarzustellen, dass die Notifikation über unterschriftsbedürftige Dokumente gegenüber Personen, die nicht auf der Plattform registriert sind, auch in Zukunft selbstverständlich durch eine Papierkopie des (nunmehr elektronisch erstellten) Originals erfolgen kann, das in der digital geführten Akte verbleibt. Einer Papierkopie des elektronischen Originals kommt exakt derselbe Informationsgehalt zu wie ein Entscheid, der eine handschriftliche Signatur trägt. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen, womit sie sich als Mehrwert zudem von dem in der Papierkopie ausgewiesenen Zeitpunkt der Erstellung des Originals überzeugen kann.

Die vorgeschlagene Lösung hätte den Vorteil, dass in einem Verfahren keine zwei Originale desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids (ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG stellt für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Aus den in Ziffer 3.1 genannten Gründen wird deshalb vorgeschlagen, einen neuen Artikel 22b einzufügen:

> ***Art. 22b*** *Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten*
>
> *Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.*

Sollte an der viel zu engen Auslegung des BEKJ festgehalten werden, die im erläuternden Bericht skizziert ist, wäre zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen, um dem in den Verfahrensgesetzen verwendeten Begriff der «Unterschrift» genüge zu tun, obwohl diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung durch das Behördensiegel ersetzt wurde.

3. Kapitel: Elektronische Übermittlung ausserhalb einer Plattform nach dem BEKJ

1. Abschnitt: Verwendung von anderen Lösungen zur Übermittlung von Dokumenten

Art. 23 Eignungsvoraussetzungen

Es ist unklar, wie das Bundesamt für Justiz den sachlichen und praktischen Anwendungsbereich von Artikel 23 gegenüber Artikel 24 abgrenzt. Dafür fehlen konkrete Beispiele.

Diese Bestimmung konkretisiert die Artikel 128b Absatz 2 der Zivilprozessordnung, Artikel 103b Absatz 2 der Strafprozessordnung und Artikel 8c Absatz 2 des Opferhilfegesetzes vom 23. März 2007. Wir gehen davon aus, dass sich diese Bestimmung an die Kommunikation zwischen Strafbehörden innerhalb der Strafprozesskette richtet, bei der Akten beispielsweise bei einem Weiterzug an die übergeordnete Instanz weitergeben müssen, wo andere Behörden mit bestimmten Verfahrenshandlungen beauftragt werden (Bsp. Ermittlungsauftrag von Staatsanwaltschaft an die Kriminalpolizei) oder bei der Übermittlung von Ergebnissen von Untersuchungshandlungen, welche die Polizei an die Staatsanwaltschaft übermittelt.

Ein zweites Anwendungsfeld ist die Zivilprozesskette, beispielsweise wenn ein Zivilgericht das Betreibungs-, das Konkursamt oder das Handelsregisteramt anweist, eine bestimmte Handlung vorzunehmen oder, wenn das erstinstanzliche Gerichte seine Akten aufgrund des Weiterzugs an die kantonale Rechtsmittelinstanz weitergibt.

Die physische Weitergabe der Akten zwischen Strafbehörden erfolgt aktuell noch oft auf dem Postweg, mit interner Post oder dem Kurierdienst. Die Beauftragung der Polizei für Untersuchungshandlung ergeht in der Regel schriftlich, jedoch werden weder genauer Zeitpunkt noch der Empfang gesondert festgehalten.

Die vorgeschlagenen Ausführungsbestimmungen orientieren sich stark an der technischen Lösung der zentralen Plattform. Bei der elektronischen Weitergabe innerhalb des Kantons (ZPO) oder unter Strafbehörden (StPO) sollten jedoch andere Anforderungen gelten als bei der Kommunikation über die zentrale Plattform.

Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank erfolgen. Dafür braucht es nach Einschätzung der Kantone keine Quittung. Die Protokollierung in den Logfiles des kantonalen IT-Systems genügen. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem mehrmaligen Versand von Dokumenten über eine externe Plattform klar vorzuziehen.

Artikel 23 sollte so ergänzt werden, damit die elektronische Weitergabe von Dokumenten durch die Mutation von Zugriffsrechten auf eine gemeinsame Datenbank zulässig ist. Die Nachvollziehbarkeit der Zeitpunkte der Übermittlung oder der Mutation von Zugriffsrechten muss gewährleistet sein. Die Anforderungen von ZPO und StPO gehen nicht so weit, dass in der digitalen Umsetzung ein synchronisierter Zeitstempel wie in Buchstabe b notwendig wäre. Deshalb ist auf dieses Kriterium zu verzichten.

Art. 24 Elektronische Übermittlung unter Behörden

Die Sachüberschrift ist zu weit gefasst und daher irreführend. Es handelt sich stets um die Kommunikation von und zu Strafbehörden oder Zivilgerichten im Rahmen von Verfahren nach StPO oder ZPO. Gleichzeitig sollte klargestellt werden, welche verfahrensleitenden und/oder verfahrensbeteiligte Behörden unter Artikel 24 fallen (vgl. dazu Art. 6 oben). Insbesondere mit Blick auf öffentlich-rechtliche Körperschaften, die nicht hoheitlich handeln, besteht insoweit Unklarheit.

Diese Bestimmung konkretisiert die Ausnahmen von Artikel 128c Absatz 2 der Zivilprozessordnung, Artikel 103c Absatz 2 der Strafprozessordnung und Artikel 8d Absatz 2 des Opferhilfegesetzes. Diese Ausnahmen sind dort sinnvoll, wo in Zivil- oder Strafverfahren eine grosse Anzahl von Kommunikationen mit Behörden anfallen, die nicht Teil der Straf- oder Zivilprozesskette sind und wo eine direkte Kommunikation, z.B. über eine Schnittstelle, etwa zur Weitergabe von Metadaten oder aus Kostengründen dem Rechtsverkehr über die Plattform vorzuziehen ist. Zu denken ist im Strafprozess etwa an Steuer- oder Migrationsbehörden oder auch an grosse Verkehrsbetriebe oder rechtsmedizinische Institute, die auch unter den Behördenbegriff fallen dürften. Ebenso bestimmte Behörden des Bundes wie das BAZG.

Die Voraussetzungen sollten sich an Artikel 23 orientieren und nicht darüber hinausgehen. Es ist jedenfalls nicht ersichtlich, weshalb Artikel 24 strengere Anforderungen vorsieht, da Artikel 103c Absatz 2 der Strafprozessordnung – anders als Art. 103b Absatz 2 mit der Feststellung der Zeitpunkte der Übermittlung und dem Schutz der Akte vor Veränderung und unberechtigter Kenntnisnahme - überhaupt keine Anforderungen an die Dokumentation einer Übermittlung stellt.

2. Abschnitt: Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Art. 25

Keine Bemerkungen.

3. Abschnitt: Elektronische Bestätigung von Protokollen im Straf- und Militärstrafprozess

Art. 26

Keine Bemerkungen.

4. Kapitel: Schlussbestimmungen

Art. 27 Aufhebung und Änderung anderer Erlasse

Keine Bemerkungen.

Art. 28 Inkrafttreten

Die geplante Gründung der Inkraftsetzung per 1. Juli 2027 wird begrüsst. Die Finanzierung des Projekts Justitia 4.0, welches die zentrale Plattform im Auftrag der Kantone, des Bundes und der Justizbehörden aufbaut, ist bis Ende Jahr 2027 gesichert. Die Finanzierung mittels Gebühren könnte bereits per 1. Juli

2027, spätestens jedoch per 1. Januar 2028 erfolgen. Die vorliegende Verordnung muss gleichzeitig mit dem abschliessendem Inkrafttreten des BEKJ in Kraft gesetzt werden.

Sollten weitere Artikel des BEKJ im Hinblick auf das Erteilen der Betriebsbewilligung vorab in Kraft gesetzt werden (siehe Bemerkungen zu Art. 3), müsste der gleiche Schritt mit den entsprechenden Bestimmungen der Verordnung erfolgen (2. Abschnitt).

Aufhebung und Änderung anderer Erlasse

Aufhebung VeÜ-VwV

Keine Bemerkungen.

Aufhebung VeÜ-ZSSV

Die Aktennotiz vom 29. April 2026 haben wir zur Kenntnis genommen. Wir begrüssen, wenn die Übergangsbestimmungen eine weitere Nutzung der bisher zugelassenen Zustellpattformen durch die Kantone ermöglichen.

Wir erachten es als kritisch, dass sich die Justizbehörden gezwungen sehen, bei Verfahren nach ZPO und StPO während einer mehrjährigen Übergangszeit zwei Kommunikationssysteme parallel zu nutzen und zu verwalten - möglicherweise mit unterschiedlichen formellen Anforderungen (qualifizierte elektronische Signatur). Die Übergangsbestimmungen sollten dahingehend harmonisiert werden, dass bereits hängige Verfahren nach neuem Recht über die Plattform geführt werden können. Wir laden das Bundesamt für Justiz ein, zusammen mit den Justizbehörden und Justitia 4.0 nach einer allseits befriedigenden Lösung zu suchen.

Art. 14a VZertES Vom Validator zu prüfende Signaturen und Siegel

Keine Bemerkungen.

Art. 14b VZertES Anbringen und validieren von elektronischer Signatur und Siegel

Keine Bemerkungen.

Par courriel adressé à

cornelia.perler@bj.admin.ch

Berne, le 15 juin 2026

Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP): procédure de consultation

Monsieur le Conseiller fédéral,

Nous vous remercions de nous avoir donné l'occasion de prendre position.

Vous trouverez dans les pages suivantes les remarques formulées dans l'optique du projet Justitia 4.0.

Nous vous remercions de la collaboration constructive avec l'Office fédéral de la justice et nous réjouissons de la finalisation réussie du projet. Nous restons à votre disposition pour toute question complémentaire.

En vous remerciant de l'accueil que vous réserverez aux observations du Projet Justitia 4.0, nous vous prions d'agréer, Monsieur le Conseiller fédéral, l'expression de notre considération la plus haute.

Yann-Eric Hofmann

Juge fédéral

Coprésident du comité de pilotage

Florian Düblin

Secrétaire général de la CCDJP

Coprésident du comité de pilotage

Commentaires, suggestions et propositions de formulation

Préambule

Le projet d'ordonnance omet délibérément de citer les articles qui confèrent au Conseil fédéral la compétence de réglementer le format des documents transmis par voie électronique. Le rapport explicatif précise que, « *pour conserver une vue d'ensemble* », le préambule ne mentionne que les dispositions des lois de procédure qui traitent de la communication en dehors des plateformes de la LPCJ. Même si une référence générale à la LPCJ semble appropriée, il serait préférable de mentionner toutes les normes de délégation contenues dans les lois de procédure. Cela vaut en particulier pour les articles qui confèrent au Conseil fédéral la compétence de définir les formats; ceux-ci devraient donc logiquement être également mentionnés dans le préambule.

Le préambule devrait dès lors être libellé comme suit:

> *vu la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ),*
>
> *vu les art. 6a, al. 2, 21a, al. 2 et 34, al. 1bis de la loi du 20 décembre 1968 sur la procédure administrative du 20 décembre 1968 (PA),*
>
> *vu l'art. 38e de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF),*
>
> *vu les art. 128b, al. 3, et 128c, al. 2 et 128e du code de procédure civile du 19 décembre 2008 (CPC),*
>
> *vu les art. 33a, al. 4, 33b, 33c, al. 2 et 34, al. 3, de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),*
>
> *vu les art. 76a, al. 2, 103b, al. 3, et 103c, al. 2 et 103e du code de procédure pénale du 5 octobre 2007 (CPP),*
>
> *vu l'art. 2e de la loi fédérale du 23 décembre 2011 sur la protection extraprocédurale des témoins (Ltém),*
>
> *vu l'art. 31f de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA),*
>
> *vu les art. 8c, al.2 et 3, et 8d, al. 2, et 8f de la loi du 23 mars 2007 sur l'aide aux victimes (LAVI),*
>
> *vu les art. 37d et 38a, al. 2, de la procédure pénale militaire du 23 mars 1979 (PPM),*

Chapitre 1 Exploitation et utilisation de plateformes

Section 1 Champ d'application

Art. 1

L'alinéa 2 concerne exclusivement les procédures qui, en vertu de la loi sur la procédure administrative (PA), relèvent du droit fédéral et **ne s'applique donc pas aux cantons**.

La valeur ajoutée de l'**alinéa 3** n'est pas évidente, étant donné qu'en cas de divergence avec une autre une loi, le principe de la *lex specialis* s'appliquerait.

Section 2 Autorisation d'exploiter

Art. 2 Conditions applicables aux plateformes

Les conditions applicables aux plateformes semblent appropriées. Compte tenu de l'évolution rapide des technologies, la taille maximale des fichiers visée à **l'alinéa 1, lettre c**, devrait être fixée dans une annexe à la présente ordonnance ou dans une ordonnance départementale du DFJP.

La fonction de suppression visée à l'alinéa 1, lettre d, est une fonctionnalité qui, le cas échéant, devrait être réglementée dans la section 3 de la présente ordonnance. Par ailleurs, la formulation de cette disposition est trop absolue et difficilement applicable. Comme le souligne à juste titre le rapport à la page 11, la fonction de suppression efface l'autorisation individuelle accordée, mais pas le document en tant que tel.

Lorsqu'un document est transmis à une autorité judiciaire ou envoyé par celle-ci, tant l'expéditeur que le destinataire ont accès au document transmis. Si, par exemple, l'expéditeur supprime son droit d'accès, le document disparaît de son profil. Le droit d'accès du destinataire reste toutefois inchangé, de sorte que le document reste visible dans son profil. Cela s'applique à toutes les personnes concernées ainsi qu'aux quittances de réception et de consultation correspondantes. La « suppression » correspond à un déplacement vers la corbeille. La suppression physique effective s'effectue en arrière-plan conformément aux dispositions légales (90 jours).

Il convient de ne pas utiliser le terme « compte utilisateur » dans le présent contexte, car celui-ci peut contenir plusieurs profils. De plus, d'un point de vue technique, les profils ne contiennent pas de documents ni de quittances, mais rendent simplement visibles les droits d'accès existants.

L'alinéa 1, lettre d, devrait donc être libellé comme suit :

> *d. les utilisateurs peuvent supprimer en tout temps les documents et quittances qui apparaissent dans le ~~compte utilisateur de~~ leur profil.*

Al. 2

Le développement des interfaces est un processus continu, et les exigences évoluent donc de manière tout aussi dynamique. Le DFJP définit les exigences fonctionnelles et opérationnelles relatives aux interfaces. Le projet Justitia 4.0 invite le DFJP, respectivement l'OFJ, à participer au forum API, où le développement des interfaces est discuté avec les utilisatrices et utilisateurs. Du point de vue du projet Justitia 4.0, la consultation de l'exploitante, telle qu'elle est évoquée dans le rapport explicatif, est indispensable.

Art. 3 Procédure d'autorisation

Dans la situation actuelle, l'autorisation d'exploitation ne pourra être délivrée qu'après l'entrée en vigueur de la LPCJ, le 1er juillet 2027. Le cas échéant, l'autorisation pourrait être délivrée immédiatement (une seconde) après l'entrée en vigueur de la LPCJ et des ordonnances. La procédure d'autorisation devrait en tout état de cause être engagée en temps utile, même si l'entrée en vigueur de la base légale n'est pas encore effective.

Il serait préférable que les articles 25, 27 et 28 de la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire soient mis en vigueur au préalable, afin que la procédure d'autorisation de la plateforme centralisée puisse démarrer en temps utile et que l'autorisation d'exploitation puisse être délivrée avant l'entrée en vigueur de l'ensemble de la loi.

En tout état de cause, il serait souhaitable que l'autorité compétente en matière d'autorisation communique les conditions requises en temps utile et coordonne la procédure d'autorisation dans la mesure nécessaire, notamment lorsque d'autres autorités ou offices fédéraux sont impliqués dans cette procédure, par exemple le PFPDT dans le domaine de la protection des données ou le service spécialisé de la sécurité relative aux entreprises du Secrétariat d'État à la politique de sécurité en vue d'une éventuelle procédure de sécurité relative aux entreprises.

Section 3 Documents, quittances et apposition d'un cachet

Art. 4 Format des documents

Le présent projet utilise – à l'instar de la LPCJ – le terme « document » plutôt que « fichier ». Le message relatif à la LPCJ (FF 2023 679, p. 20) justifie ce choix en invoquant que le terme « fichier » est un terme trop technique pour être utilisé dans la loi.

En ce sens, il serait préférable d'utiliser le terme « fichier » dans l'ordonnance, dans la mesure où il s'agit d'aspects techniques des pièces transmises.

Al. 1

Nous sommes favorables à la définition du format PDF/A pour les documents des autorités et des formats PDF et PDF/A pour les autres participants à la procédure.

Al. 2

Dans de nombreux cas, le format PDF suffit pour reproduire le contenu informatif d'un document de manière juridiquement valable. Dans ces cas, les pièces doivent être déposées dans ce format largement répandu. Cela facilite le traitement des dossiers par les avocats, les ministères publics, les tribunaux, les autorités administratives et les autres parties à la procédure. Si les parties soumettent leurs pièces jointes au format PDF, la conversion par les autorités judiciaires n'est plus nécessaire et toutes les parties disposent du même document. La numérisation vise à accélérer les procédures et à simplifier la gestion des dossiers. Si en règle générale les documents sont disponibles au format PDF, cela permet un traitement rapide par les avocats et les autorités. Pour des raisons de sécurité, les systèmes de gestion des dossiers des avocats et des autorités ne peuvent traiter qu'un nombre limité de types de fichiers (« White-listening » des formats de fichiers). Si le format des pièces jointes pouvait être choisi librement, cela compliquerait considérablement le traitement des dossiers. Toutes les parties à la procédure devraient d'abord rechercher le programme approprié pour ouvrir un fichier. De plus, le choix illimité des formats constituerait un risque considérable pour la sécurité informatique de toutes les parties concernées.

Dans certains cas particuliers, le format PDF ne permet pas de restituer suffisamment le contenu informatif d'un document. On peut penser par exemple à des enregistrements audio ou vidéo, à des vidéosurveillances multipistes de tunnels ou à des enregistrements provenant de voitures électriques. Dans ces cas, le DFJP devrait définir quels formats de fichiers peuvent être transmis directement via la plateforme. Pour des raisons de sécurité, la plateforme analyse tous les fichiers pour détecter des virus. Ce faisant, la plateforme ne peut en principe analyser de manière efficace que les formats de fichiers qu'elle connaît. Pour les documents qui ne peuvent pas être transmis directement via la plateforme, il est possible de les transmettre dans un conteneur, par exemple au format Zip.

Les formats de fichiers que la plateforme doit prendre en charge doivent être définis par le DFJP dans une ordonnance départementale, après consultation de l'exploitant de la plateforme centralisée.

L'alinéa 2 devrait donc être libellé comme suit :

> [2] ~~*Les annexes peuvent être remises dans n'importe quel format*~~ *Si le format PDF ne permet pas de restituer correctement le contenu d'un document, l'annexe peut être transmise dans son format d'origine*.

Al. 3 et 4

La sélection proposée de formats de fichiers est adéquate, mais le niveau de norme retenu est critiquable. La définition des formats que les autorités qui dirigent la procédure doivent traiter devrait figurer dans une annexe à l'OCEP ou dans une ordonnance départementale du DFJP.

La liste des formats de documents pris en charge est en constante évolution. Il faut donc s'attendre à des adaptations fréquentes. De plus, la simple mention des formats de documents dans l'ordonnance n'est pas suffisante. D'autres détails techniques, tels que le traitement des fichiers protégés par mot de passe ou cryptés, doivent être réglementés, y compris, le cas échéant, les éléments individuels d'un fichier ouvert qui sont néanmoins cryptés ou protégés par mot de passe (par exemple, les macros dans un fichier

Microsoft Excel, les fichiers ZIP contenant des fichiers partiellement cryptés, etc.). Il est nettement plus facile de gérer cela dans une annexe que dans le corps de la présente ordonnance.

Les alinéas 3 et 4 devraient donc être libellés comme suit:

> [3] ~~*L'autorité qui dirige la procédure doit pouvoir traiter les formats suivants :*~~
>
> ~~*a. documents écrits : PDF, PDF/A ;*~~
>
> ~~*b. images : BMP, GIF, JPEG, PNG ;*~~
>
> ~~*c. fichiers audio : MP3, OGG, WAV ;*~~
>
> ~~*d. fichiers vidéo : AVI, MOV, MKV, MP4 ;*~~
>
> ~~*e. fichiers d'archives : ZIP, 7z.*~~
>
> *Si l'autorité qui dirige la procédure ne peut ouvrir une pièce jointe dans le format dans lequel elle a été transmise, elle accorde à la partie qui l'a transmise un délai approprié pour qu'elle puisse la transmettre dans un format défini par l'autorité.*
>
> [4] ~~*Lorsqu'une annexe a été remise dans un autre format et que l'autorité qui dirige la procédure ne peut pas la traiter de manière appropriée, l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée*~~ *Le DFJP définit les formats de fichiers à transmettre via la plateforme.*
>
> [5] ~~*L'autorité qui dirige la procédure fixe un délai approprié.*~~

Art. 5 Quittances

La plateforme centralisée appose un cachet sur les quittances des utilisateurs, qu'ils transmettent un ou plusieurs documents.

La réglementation proposée est globalement adéquate. Les communications électroniques via la plateforme ne nécessitent pas de signature. Les autorités peuvent être identifiées grâce à leur cachet individuel, qu'elles apposent sur leurs documents avant leur transmission électronique. Les personnes physiques sont identifiées via AGOV. Les organisations, en revanche, ne disposent pas d'identifiants électroniques. Elles sont identifiées par l'intermédiaire des personnes physiques qui agissent en tant qu'organe ou mandataires de l'organisation. En conséquence, tout profil sur la plateforme centrale qui n'appartient pas à une autorité est associé à une personne physique en tant que personne responsable.

Le projet d'ordonnance formule les dispositions relatives aux quittances de réception du point de vue de l'utilisateur (« expéditeur », « destinataire »). Le projet Justitia 4.0 propose de formuler ces dispositions de manière plus précise, en s'alignant sur la configuration technique actuelle. Selon nous, cela apporte davantage de clarté aux utilisateurs, car les termes utilisés dans l'ordonnance se retrouvent, par exemple, également dans le formulaire de saisie de la plateforme justitia.swiss.

L'autorité étant suffisamment identifiée par son cachet, **le nom de la personne responsable du profil d'une autorité**, conformément à l'al. 2, let. b, ne doit, à juste titre, **pas** figurer sur la quittance. Seul le nom de l'autorité doit apparaître sur la quittance de réception.

L'article 24, alinéa 4, de la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire prévoit que le cachet électronique réglementé apposé ne contient pas d'information sur l'attribution d'un droit. De l'avis du projet Justitia 4.0, il en va de même pour les quittances. L'attribution d'un droit ne doit pas être visible sur la quittance.

La quittance doit donc mentionner le nom du profil au nom duquel l'envoi est effectué, ainsi que le nom de la personne responsable (alinéa 2, lettre b).

L'alinéa 2, let. d, précise les modalités de la quittance de réception et stipule notamment que les informations relatives aux documents non transmis doivent figurer sur ladite quittance. Les motifs possibles conduisant au rejet d'un document peuvent être un résultat positif au test antivirus, la taille du fichier ou un format de fichier non pris en charge par la plateforme. Cette disposition comporte une erreur logique. Les documents non transmis ne peuvent pas figurer sur la **quittance de réception**, puisqu'ils n'ont justement **pas été transmis**. Par conséquent, la quittance ne peut contenir la valeur de hachage de fichiers qui n'ont pas été transmis. Si la plateforme ne parvient pas à transmettre un ou plusieurs documents, l'expéditeur reçoit un message de la plateforme, mais pas de quittance. Le chiffre 2 doit donc être adapté comme suit:

[2] Les quittances comportent en particulier les données suivantes :

a. le type de quittance ;

b. le nom ~~de l'~~ profil expéditeur, son adresse sur la plateforme et ~~le cas échéant~~ le nom de la personne responsable ~~l'organisation ou de l'entreprise pour laquelle il agit~~;

c. le nom du profil destinataire ~~ou de son entreprise et~~ son adresse sur la plateforme ;

d. pour la quittance de réception :

1. la liste des documents transmis, leur taille et leur valeur de hachage,

~~2. la liste des documents qui n'ont pas été transmis en raison du résultat du contrôle antivirus, avec indication de leur taille,~~

~~3.~~2. le moment de la transmission à la plateforme ;

e. pour la quittance de consultation, le moment de la première consultation ;

f. pour la quittance de non-consultation, le moment de la transmission à la plateforme ;

g. lors de l'envoi ou de la première consultation d'un document par une personne à laquelle ces droits ont été transférés, le nom ~~de la personne~~ du profil au nom duquel ~~de laquelle~~ le document a été envoyé ou consulté.

Les plateformes doivent à l'avenir pouvoir également transmettre des données structurées, par exemple sous forme de fichiers XML. Les exceptions prévues aux alinéas 4 et 5 sont donc essentielles, car les fichiers XML, pour des raisons techniques, ne peuvent pas être cachetés.

Art. 6 Apposition d'un cachet par l'autorité expéditrice

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme ; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement. La plateforme au contraire appose un cachet **après** la transmission à la plateforme, sur la quittance de réception émise sur la base de l'article 5.

L'article 6 règle **l'apposition d'un cachet sur les documents** par l'autorité dirigeant la procédure **avant leur transmission via une plateforme** (art. 22 al. 2 LPCJ). Le projet d'ordonnance mentionne que lorsque plusieurs documents sont transmis, il suffit que l'un des de ces documents soit muni d'un cachet, ce qui est correct. On ajoutera que l'apposition d'un cachet par l'autorité qui dirige la procédure a lieu indépendamment du nombre de documents transmis. Même si un seul document est transmis par l'autorité qui dirige la procédure, celui-ci doit être muni d'un cachet, afin que l'authenticité du document puisse être examinée indépendamment de la plateforme.

Les explications figurant dans le rapport explicatif, selon lesquelles une autorité doit apposer un cachet électronique sur tous les documents, contredisent le libellé de l'ordonnance. L'apposition d'un cachet sur un seul document par l'autorité qui dirige la procédure suffit. Par ailleurs l'obligation d'apposer un cachet imposée aux autorités qui dirigent la procédure ainsi qu'aux autorités qui y participent est en contradiction avec le concept technique de la plateforme centralisée.

Pour diverses fonctionnalités qui ont déjà été développées et mises en œuvre sur la plateforme centralisée, **la distinction entre les autorités qui dirigent la procédure et les autorités participant à la procédure** est essentielle. Ainsi, seules les autorités qui dirigent la procédure peuvent procéder à des notifications. Seules les adresse des autorités qui dirigent la procédure sont visibles pour les tiers dans le registre public de la plateforme. Si l'obligation d'apposer un cachet était maintenue pour les autorités qui dirigent la procédure **et** celles participant à la procédure, toutes les autorités pourraient effectuer sans restriction des notifications à d'autres autorités, organisations et particuliers et indépendamment d'une procédure (judicaire). Cela ouvrirait la plateforme à toute communication électronique entre autorités, pour laquelle la LPCJ n'offre toutefois pas de base légale suffisante. L'objectif de la LPCJ est de permettre la communication électronique dans le cadre des procédures judiciaires.

Seules les autorités qui dirigent la procédure sont tenues d'apposer un cachet électronique sur leurs documents. L'article 22, alinéa 2, LPCJ doit donc être interprété de manière restrictive. Le cachet électronique garantit l'origine, la date exacte, l'intégrité et l'authenticité du document muni d'un cachet. La décision incidente ou le jugement d'une autorité qui dirige la procédure crée des droits et des obligations. Ceux-ci produisent leurs effets au-delà de la procédure en cause. Les personnes concernées doivent donc pouvoir vérifier, indépendamment d'une procédure concrète ou de la plateforme centralisée, si le document en question est intègre et authentique et s'il a été établi par l'autorité compétente. En résumé, le cachet électronique est nécessaire précisément là où les autorités agissent de manière autoritaire.

Les autorités participant à la procédure ne peuvent en revanche pas être tenues d'apposer un cachet électronique sur leurs documents. Les documents que les autorités parties à la procédure transmettent dans le cadre d'une procédure judiciaire ne créent généralement pas de nouveaux droits et obligations. Il s'agit généralement d'extraits de registres existants, d'extraits de dossiers existants de procédures antérieures ou de décisions déjà notifiées issues de procédures closes, qui sont désormais mis à disposition pour une procédure judiciaire. L'authentification sur la plateforme permet l'identification correcte de l'autorité. Si une partie à la procédure souhaite contester l'intégrité ou l'authenticité d'un document transmis par une autorité partie à la procédure, il s'agit d'une question d'appréciation des preuves dans la procédure correspondante.

Si l'obligation d'apposer un cachet était maintenue pour toutes les autorités conformément au rapport, toutes les autorités suisses devraient être équipées d'un cachet à tous les niveaux. La LPCJ n'offre pas de base légale suffisante pour équiper l'ensemble des autorités suisses d'un cachet électronique. L'instauration généralisée d'un cachet électronique entraînerait pour les cantons un effort organisationnel considérable et des coûts importants.

Selon le rapport explicatif, il n'y aurait plus lieu d'apposer un cachet sur les documents dotés d'une signature électronique qualifiée. Cette affirmation ne correspond ni au concept de la LPCJ, ni à la mise en œuvre actuelle par la plateforme centralisée. La LPCJ ne prescrit aucune fonctionnalité permettant à la plateforme centralisée de contrôler quelles signatures électroniques qualifiées sont attribuées à une autorité donnée.

Etant donné que l'identification d'une autorité se fait par le biais du cachet électronique, la plateforme centralisée ne dispose à ce jour d'aucune fonctionnalité lui permettant de contrôler les signatures électroniques ou d'attribuer des signatures à une autorité ou à une organisation. C'est pourquoi les autorités dirigeant la procédure doivent également apposer un cachet sur les documents déjà munis d'une signature électronique qualifiée avant de les transmettre via la plateforme.

Du point de vue du projet Justitia 4.0, il est important de souligner la différence entre la notification et la consultation en ligne de documents. Contrairement à ce qui est le cas pour une notification et comme l'explique le rapport explicatif, il n'y a pas d'obligation pour l'autorité qui dirige la procédure d'apposer son cachet sur les documents lors de la consultation en ligne du dossier.

Art. 7 Apposition d'un cachet par la plateforme

Dans le cadre de la communication électronique dans le domaine judiciaire, le cachet électronique devra désormais être apposé à deux étapes distinctes. L'autorité qui dirige la procédure appose son cachet sur l'un des documents transmis **avant** leur envoi à la plateforme ; il s'agit généralement de la décision, de l'arrêt ou de la lettre d'accompagnement (art. 6). L'article 7, en revanche, fait référence à l'apposition d'un cachet sur la quittance **après** sa transmission par la plateforme centrale.

Al. 1

Ce principe se fonde sur l'article 2, lettre a, de la loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (SCSE). Selon cette disposition, une signature électronique désigne ensemble de données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité.

Le principe de l'apposition du cachet électronique par la plateforme a été correctement repris: le support du cachet électronique de la plateforme est la **quittance, jamais le document ou le fichier transmis.** Dans le cas de la plateforme centralisée, le document distinct visé à l'article 7, alinéa 1, est la quittance de réception ou la quittance de consultation. La plateforme appose son cachet électronique sur la quittance de réception des utilisateurs, qu'ils transmettent un ou plusieurs documents. L'alinéa 1 devrait donc être libellé comme suit :

> [1] *Lorsque ~~plusieurs~~ des documents sont transmis, la plateforme appose le cachet et l'horodatage sur un document séparé. Le document mentionnera le nom, la taille et la valeur de hachage de chaque document transmis.*

Al. 2

L'alinéa 1 décrit le cachet électronique apposé sur les quittances. La transmission de documents munis d'un cachet suit les mêmes règles que celles de l'alinéa 1. **L'alinéa 2 doit donc être supprimé**.

> ~~[2] *Les documents qui sont déjà munis d'un cachet ou d'une signature électronique qualifiée et d'un horodatage ne doivent pas être munis d'un cachet supplémentaire.*~~

Section 4: Authentification, profils, interfaces et attribution de droits

Art. 8 Authentification des utilisateurs

L'authentification via AGOV conformément à l'alinéa 1 est, de notre point de vue, jugée judicieuse et pertinente. Les exigences détaillées devraient être fixées dans une ordonnance du DFJP.

L'utilisation éventuelle de services d'authentification supplémentaires dans le cadre de futures plateformes cantonales, conformément à l'alinéa 2, est jugée adéquate.

À l'avenir, la plupart des autorités seront reliées à la plateforme via une interface. La disposition proposée à l'alinéa 3 laisse une marge de manœuvre suffisante pour mettre en œuvre de futures solutions techniques.

Art. 9 Profils

Dans la mise en œuvre actuelle de la plateforme, à chaque profil (autre que celui d'une autorité) est attribué une personne physique disposant de son propre compte d'utilisateur, en tant que personne respon-

sable. Le nom de la personne responsable apparaît dans le répertoire d'adresses de la plateforme centralisée, visible pour les autorités, ainsi que sur les quittances émises. Dans le répertoire d'adresses public, en revanche, seules les adresses des autorités chargées de la procédure sont visibles.

Le nom de la personne responsable permet d'identifier l'organisation au nom de laquelle elle agit. La personne responsable peut ajouter au profil dont elle a la charge d'autres membres disposant de leur propre compte utilisateur. Le nom des autres membres n'apparaît ni dans le régistre ni sur les quittances. La personne responsable est régulièrement invitée à vérifier les autorisations des membres invités. La personne responsable peut transférer son rôle à un autre utilisateur.

Dans un profil d'autorité le nom de la personne responsable n'apparaît ni dans le registre des adresses, ni sur les quittances.

Al. 1

La formulation de l'alinéa 1 est très absolue et ne tient pas suffisamment compte des particularités du profil d'autorité. Elle pourrait également prêter à confusion, car la systématique du texte (alinéa 1) donne l'impression que tout utilisateur pourrait créer un profil d'autorité sans autres conditions. Il est proposé de déplacer l'alinéa 1 à la fin de l'article 9.

Pour les autres utilisateurs, l'alinéa 1 correspond à la mise en œuvre actuelle par la plateforme centralisée, selon laquelle chaque utilisateur peut créer plusieurs profils. À l'inverse, chaque profil (qui n'est pas une autorité) repose sur le compte d'utilisateur d'une personne physique.

Al. 2

Cette disposition se réfère uniquement aux autorités qui dirigent la procédure, qui figurent également dans le registre (public) des adresses de la plateforme. Dans le cas des autorités qui dirigent la procédure, il convient de renoncer à l'indication d'une adresse postale, étant donné que, selon le projet Justitia 4.0, la recherche de l'adresse d'une administration ne s'effectue pas via le registre des adresses de la plateforme, mais via le site web de l'administration concernée. Si nécessaire, un complément ou le lieu peuvent être ajoutés au nom de l'autorité. Le répertoire des plateformes de notification actuellement reconnues (Inca-Mail et PrivaSphere) ne contient ni adresses privées ni adresses professionnelles. La disposition doit être adaptée en conséquence:

> *2 Les profils des autorités comprennent au moins les données suivantes :*
>
> *a. le nom de l'autorité ;*
>
> *~~b. l'adresse postale ;~~*
>
> *b ~~c.~~ ~~le nom~~ la désignation du cachet.*

Al. 3

La reprise de la date de naissance à partir du compte AGOV est déjà envisagée par la plateforme centralisée. Selon la mise en œuvre actuelle, la date de naissance sert à identifier une personne physique. Il n'est toutefois pas techniquement possible de rechercher des utilisateurs sur la base de leur date de naissance.

Il convient de souligner que l'adresse privée n'est pas mise à jour dans le compte AGOV. L'exactitude de l'adresse privée repose sur la déclaration de l'utilisateur. Elle n'est pas vérifiée lors de l'identification, ce qui la rend peu fiable. Du point de vue de la protection des données également, l'enregistrement de l'adresse privée dans les profils d'utilisateurs doit être considéré comme critique**. Il convient donc de renoncer** à la collecte des adresses postales des personnes physiques.

Les organisations ont des structures variées et, le cas échéant, des succursales différentes, raison pour laquelle le profil numérique utilisé ne doit pas nécessairement correspondre à l'adresse postale. Cette

dernière n'apporte aucune valeur ajoutée notable dans le cadre de la notification numérique**. Il convient donc de renoncer à l'adresse postale également pour les organisations.**

Während verfahrensleitende Behörden über ihr Siegel identifiziert werden, erfolgt die Identifikation von Organisationen über die verantwortliche Person, welche dem Profil der Organisation zwingend zugeordnet ist. Der Name der verantwortlichen Person soll daher im Profil und im Verzeichnis der Plattform ersichtlich sein.

L'alinéa devrait donc être formulé comme suit:

> *3 Les profils des autres utilisateurs comprennent au moins les données suivantes :*
>
> *a. pour les personnes physiques : le prénom, le nom, et la date de naissance ~~et l'adresse postale~~ ; …*
> *b. pour les organisations : le nom de l'organisation ou de l'entreprise ~~et l'adresse postale.~~*

Al. 4

Selon l'interprétation de Justitia 4.0, l'alinéa 4 concerne la communication entre les représentants professionnels et l'autorité qui dirige la procédure. D'après le libellé, cette disposition ne s'applique qu'aux avocats exerçant pour le compte d'une organisation. Il n'est pas clair si les représentants de parties exerçant seuls ou qui partage simplement un bureau commun doivent également porter une mention supplémentaire afin d'être identifiables en tant que tels. Grâce à l'introduction de la notion de « personne responsable », le profil et la quittance correspondante permettent de déterminer quelle personne physique agit. Il est donc possible de se passer de l'alinéa 4.

Il serait préférable de prévoir un champ facultatif permettant d'ajouter une précision sous forme de texte libre, par exemple : «avocate ou étude de la rue du cerf ». Cela serait possible, car le paragraphe 3 ne fixe que les informations minimales requises.

Art. 10 Interface

Cet article permet aux utilisateurs de la plateforme de connecter leurs systèmes à celle-ci via une interface et d'octroyer des droits de représentation à leurs collaborateurs. Cela se fait par l'intermédiaire d'un utilisateur technique qui reçoit un mot de passe numérique (token). La réglementation proposée est jugée adéquate par le projet Justitia 4.0.

Art. 11 ~~Attribution~~ Confirmation et retrait de droits

La réglementation proposée à l'alinéa 1 est adéquate et peut être mise en œuvre sur la plateforme. Dans la version française, il conviendrait de parler de « confirmation » plutôt que d'« attribution ».

Nous sommes favorables à la variante proposée à l'alinéa 2.

Section 5: Protection des données, sécurité des données et contrôle antivirus

Art. 12 Durée maximale de conservation des documents et des quittances

L'article 12 prévoit la destruction automatique des documents et des quittances sur la plateforme à l'expiration d'un délai de six mois à compter de leur création. La suppression automatisée des documents et des quittances après un délai raisonnable est adéquate, d'autant plus que la plateforme est conçue comme une « boîte aux lettres » et non comme un système d'archivage à long terme. Pour des raisons d'uniformité et de minimisation des données, le projet Justitia 4.0 approuve la solution proposée.

Art. 13 Sécurité des données

La disposition proposée renvoie à la section 3; la mention du chapitre pertinent (2 ?) fait défaut et devrait être ajoutée. De plus, la première référence à la disposition de l'ordonnance est incomplète.

L'article 13 devrait donc être formulé comme suit:

> *La sécurité des données sur les plateformes visées à l'art. 1, al. 1, let. b, mises à disposition par les cantons est régie par la section 3, chapitre X de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information et par l'art. 8 de la loi du 25 septembre 2020 sur la protection des données.*

Art. 14 Contrôle antivirus

Du point de vue technique, il convient de distinguer trois cas dans le cadre de l'analyse prévue visant à détecter les logiciels malveillants.

1. Analyse complète des fichiers transmis : la taille maximale de chaque fichier ne doit pas dépasser une limite supérieure définie, faute de quoi le logiciel d'analyse atteindrait sa limite (espace de stockage, etc.), interromprait l'analyse et le processus d'analyse pourrait prendre tellement de temps que le respect des délais serait compromis en cas de soumission dans l'urgence.

2. Analyse limitée des fichiers volumineux : un fichier qui dépasse la taille maximale fixée est divisé en blocs gérables aux fins de l'analyse de logiciels malveillants, lesquels sont ensuite analysés individuellement. Cette procédure est toutefois moins fiable que l'analyse complète. Les logiciels malveillants qui, du fait de la division en blocs vérifiables, sont répartis sur deux blocs consécutifs, peuvent ne plus être détectés comme logiciels malveillants. Cela doit être clairement indiqué aux utilisatrices et utilisateurs de la plateforme. Il convient notamment de signaler clairement au destinataire qu'il doit **effectuer son propre contrôle complet de la présence de logiciels malveillants sur les données stockées localement après le téléchargement du fichier**.

3. Renonciation au contrôle antivirus : lors de la phase pilote de la plateforme, il est apparu que les mesures de protection mises en place sont, dans certains cas, trop strictes. Les raisons suivantes (liste non exhaustive) ont été identifiées :

   - Transmission de preuves électroniques provenant d'appareils saisis, dans leur version originale ou après avoir été traitées par la police scientifique (forensique informatique), par exemple dans le cadre de la consultation du dossier.
   - Transmission de fichiers protégés par mot de passe ou chiffrés de bout en bout entre certaines autorités. Ces fichiers ne peuvent en principe pas être analysés pour détecter de logiciels malveillants, car ils sont chiffrés.
   - Transmission de formats de fichiers contenant des macros ou d'autres codes exécutables. Bien qu'ils ne contiennent pas de virus au sens classique du terme, ils offrent de nombreuses possibilités d'attaque pour les cybercriminels. C'est pourquoi les formats de fichiers exécutables sont rejetés par la plateforme pilote.
   - En raison des mesures de protection prises, des fichiers sont rejetés à tort, bien qu'ils aient été nettoyés par les autorités expéditrices. Ce comportement est appelé « faux positifs ».

Au cours de la phase pilote, il a été demandé à plusieurs reprises de pouvoir également transmettre de tels fichiers et de ne pas avoir à recourir à des moyens de transmission alternatifs (non sécurisés) (e-mail classique, cloud, clés USB, etc.). Le stockage et la récupération de ces documents, y compris les éventuelles vérifications de la présence de logiciels malveillants, incombent dans ce cas aux utilisateurs de la plateforme. Si l'expéditeur et le destinataire souhaitent contourner les mesures de protection, ils réduisent la fonction de la plateforme à la simple transmission de données et sont eux-mêmes responsables de la gestion correcte des fichiers. Cela nécessite un accord entre les parties concernées. Et **cela signifie également que les utilisateurs doivent effectuer leur propre analyse antivirus complète des données stockées localement, respectivement avant et après leur transmission via la plateforme**. La plateforme doit en outre signaler au destinataire que les fichiers transmis dans un conteneur n'ont pas été soumis à une analyse antivirus. Il incombe en outre à l'utilisateur de placer les fichiers

à transférer dans un format conteneur pris en charge par la plateforme. À l'heure actuelle, la plateforme ne propose pas cette fonctionnalité.

Al. 1

La définition de la taille des blocs vérifiables pour les fichiers volumineux ne devrait pas être communiquée publiquement. Cette information n'est pas pertinente pour les utilisateurs de la plateforme. Elle offre aux attaquants potentiels la possibilité de diffuser leurs logiciels malveillants dans un fichier infecté de telle sorte que, lors du fractionnement en blocs, le code malveillant se trouve dans deux blocs consécutifs et ne puisse pas être détecté de manière fiable comme étant nuisible. De plus, la taille de ces blocs dépendra fortement du logiciel chargé de la division et de la vérification. Cette limite évoluera également de manière dynamique en fonction de l'expérience opérationnelle et des améliorations apportées au matériel et aux logiciels, et devrait pouvoir être facilement adaptée.

L'alinéa 1 devrait donc être libellé comme suit:

> [1] *Les plateformes ~~soumettent les documents ayant une taille maximale de 64 mégaoc tets à~~ effectuent un contrôle antivirus.*

Al. 2

La limite actuelle de 64 Mo pour un contrôle complet des logiciels malveillants peut (et devrait) être facilement augmentée par les exploitants de la plateforme en fonction des possibilités techniques et de l'expérience opérationnelle croissante. **L'alinéa 2 doit donc être supprimé**.

> ~~[2] Elles peuvent diviser les documents dépassant 64 mégaoctets en plusieurs documents de 64 mégaoctets au plus et soumettre ceux-ci à un contrôle antivirus.~~

Al. 3

La renonciation au contrôle antivirus est étroitement liée aux formats de documents autorisés (art. 4). Les documents que la plateforme centralisée ne peut pas transmettre en raison de leur format ou qui ont été détectés à tort comme positifs lors du contrôle antivirus peuvent être transmis dans un conteneur, à condition que l'expéditeur et le destinataire consentent à cette transmission.

Al. 4

Une déclaration claire, lorsque le dépistage des virus n'a été effectué que de manière limitée, est essentielle selon nous. La manière dont les résultats du dépistage des virus sont communiqués aux utilisateurs n'est pas claire. Cette communication doit être simple sur le plan technique et facile à comprendre sur le fond.

L'alinéa 4 devrait donc être libellé comme suit:

> [4] Les documents qui n'ont pas été soumis à un contrôle antivirus ~~au sens de l'al. 2 ou~~ ou qui ont été soumis à un contrôle antivirus limité doivent être identifiés en tant que tels.

Al. 5

Lorsque la plateforme informe l'expéditeur qu'un document n'a pas pu être transmis, il ne s'agit manifestement pas d'une quittance, puisqu'aucun document n'a été transmis (voir les commentaires aux art. 5, al. 2, let. d, ch. 2, ci-dessus).

Pour les avocats, il est important que le rejet de documents par la plateforme soit dûment documenté. Actuellement, l'équipe de Justitia 4.0 élabore une première solution permettant à l'utilisateur ou à l'utilisatrice d'enregistrer l'affichage du message d'erreur en cas de non-transmission d'un document.

Section 6 Émolument pour l'utilisation de la plateforme centralisée

Le calcul des émoluments se fonde sur les articles 6 et 32 de la LPCJ. Les coûts de la plateforme sont répartis entre les cantons utilisateurs. Pour les membres de la corporation, la part des émoluments est calculée sur la base de la population résidante permanente. Avec les non-membres, la corporation conclut une convention conformément à l'article 6 de la LPCJ. L'indemnisation convenue doit couvrir l'ensemble des frais (y compris les frais d'investissement, FF 2023 679, p. 22) occasionnés par les non-membres. Les coûts pour les non-membres seront donc généralement plus élevés que ceux des membres.

Art. 15 Calcul de l'émolument

Les versions allemande et française ont été comparées et harmonisées; cela vaut également pour la cohérence terminologique des notions y figurant. Pour plus de clarté, l'alinéa 1 a été scindé en deux (nouveaux) alinéas.

La référence à la planification financière triennale pour la fixation du montant total de l'émolument pour trois ans est saluée. Cette approche fournit une base prévisible et réaliste pour l'émolument fixé annuellement selon la clé de répartition figurant à l'article 16. Au surplus, la mesure corrective prévue à l'alinéa 4 garantit une capacité d'adapter l'émolument si nécessaire.

Le texte suivant est proposé:

[1] Le montant total de l'émolument annuel dû ~~pour l'utilisation de la plateforme centralisée couvre les frais d'exploitation et de développement de la plateforme~~ par les membres de la corporation de droit public doit couvrir les frais d'exploitation et de développement ~~de la plateforme centralisée~~ et permet la constitution d'une réserve correspondant à 10 % des frais d'exploitation annuels pour assurer la liquidité de la corporation de droit public. ~~Les recettes versées par les cantons qui ne sont pas membres de la corporation pour les prestations auxquelles ils recourent sont déduites du calcul du montant total de l'émolument~~.

[2] Les contributions versées par les cantons qui ne sont pas membres de la corporation de droit public sont déduites du montant total de l'émolument.

[3]Le DFJP fixe le montant ~~annuel~~ total de l'émolument annuel à l'avance, tous les trois ans ~~en se fondant~~ sur la base de la planification financière de la corporation de droit public.

[34] Le DFJP peut adapter l'émolument pendant la période visée à l'al. ~~2~~ 3 s'il constate que les contributions encaissées par la corporation au sens des al. 1 et 2 ~~il~~ ne couvrent pas les frais d'exploitation et de développement de la plateforme ou que la réserve dépasse la limite fixée à l'al. 1.

Art. 16 Répartition de l'émolument

Selon l'état actuel de la planification, l'administration fédérale utilise la plateforme pour les procédures pénales administratives de la Confédération, mais pas pour les procédures administratives de première instance. La part fédérale de 10 % est donc jugée appropriée. Une fois l'obligation pleinement mise en œuvre, il conviendra d'examiner si l'utilisation effective correspond au modèle d'émolument proposé ou s'il y a lieu d'adapter la répartition des émoluments, notamment au regard du nombre de transmissions relevant du droit pénal administratif. Une révision du mode de calcul de l'émolument est d'ailleurs prévue à l'article 21. La répartition de l'émolument devrait également faire l'objet d'un examen.

Nous sommes favorables à la répartition en fonction de la population résidente permanente prévue à l'alinéa 2. Toutefois, seules les données statistiques disponibles au moment du calcul peuvent servir de base. Sur la base de ces données contraignantes, le DFJP fixe le montant annuel des émoluments; il tient compte à cet égard des seuils définis à l'article 15, alinéa 4, ainsi que de l'adhésion éventuelle d'un non-membre à la corporation justitia.swiss après sa création (cf. art. 19 de la convention justitia.swiss ainsi que le rapport explicatif relatif à la convention justitia.swiss, p. 17).

La formulation suivante est proposée:

[1] Le montant total de l'émolument est réparti comme suit entre la Confédération et les cantons membres de la corporation de droit public :

a. administration fédérale et Ministère public de la Confédération (MPC) : 5 % ;

b. tribunaux de la Confédération : 5 % ;

c. cantons : 90 %.

[2] La part des cantons est répartie entre les cantons qui sont membres de la corporation public proportionnellement à leur population résidente permanente au ~~moment de la fixation de l'émolument~~ 1er janvier de l'avant-dernière année pour laquelle l'émolument est dû ; est déterminant le nombre d'habitants selon la loi fédérale du 9 octobre 1992 sur la statistique fédérale, la loi du 22 juin 2007 sur le recensement et les ordonnances qui s'y rapportent.

[3] Le DFJP fixe chaque année la répartition de la taxe entre les cantons.

Art. 17 Part de l'administration fédérale et du MPC

Aucune remarque.

Art. 18 Part des tribunaux de la Confédération

Aucune remarque.

Art. 19 Échéance

L'ordonnance laisse ouvertes les autres modalités d'exécution. On peut supposer que les règles du code des obligations s'appliquent par analogie. Il est donc proposé d'adopter le libellé suivant pour cette disposition:

[1] L'émolument annuel ~~facturé aux~~ des membres de la corporation de droit public doit être versé à l'avance et est dû le 1er janvier.

[2] L'émolument ~~pour la première année d'exploitation de la corporation de droit public est dû le jour de l'entrée en vigueur~~ pour l'utilisation de la plateforme centrale est dû pour la première fois à la date d'entrée en vigueur de la présente ordonnance.

[3] Les dispositions du Code des obligations relatives à la demeure du débiteur s'appliquent par analogie.

Art. 20 Service comptable cantonal

Aucune remarque.

Art. 21 Évaluation des règles de calcul de l'émolument

Nous sommes favorables à la révision du mode de calcul de l'émolument.

Chapitre 2 Numérisation et renvoi de documents physiques et notification de copies papier de documents originaux générés par voie électronique

Art. 22

D'une manière générale cette disposition semble adéquate.

Le format PDF/A prescrit à l'alinéa 2 facilite l'archivage des dossiers judiciaires. Il n'est toutefois pas certain que ce format puisse être facilement traité par les applications judiciaires cantonales, qui sont très différentes les unes des autres.

L'alinéa 3 prévoit la reconnaissance de texte. Celle-ci semble judicieuse dans de nombreux cas et facilite le traitement des documents. Pour les textes en langue étrangère, le résultat de la reconnaissance de texte peut toutefois s'avérer insatisfaisant ou erroné selon l'état actuel de la technique. Selon Justitia 4.0, la résolution (DPI) ne devrait pas être fixée de manière rigide dans l'ordonnance. La résolution optimale en DPI dépend fortement du document original concerné. Pour les documents texte classiques, une résolution de 150 DPI est généralement suffisante, tandis qu'il peut être judicieux de numériser les images avec une résolution plus élevée.

Art. 22*a* **Renvoi de documents physiques (nouveau)**

Problématique

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est indiqué qu'il a été renoncé à intégrer dans l'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (P-OCEP) une disposition relative à l'interprétation restrictive de l'article 30 LPCJ, car il n'y avait plus de marge de manœuvre légale à cet effet.

Cette constatation se réfère à l'interprétation de la notion de « documents » contenue dans l'article 30 de la LPCJ, qui n'est distinguée dans la loi ni par domaine juridique ni par contenu des documents. Une approche différenciée est toutefois nécessaire, selon l'avis défendu ici, afin de ne pas créer, avec une ordonnance lacunaire relative à la LPCJ, des problèmes qui n'existent pas encore dans le monde analogique. Cela signifie également que, selon l'avis défendu ici, les lois de procédure applicables laissent tout à fait une marge d'interprétation des dispositions de la LPCJ dans le sens de leur objectif législatif.

En particulier dans la procédure pénale, les documents déposés physiquement ne sont renvoyés à leur expéditeur que dans des cas exceptionnels. Les services de police et les ministères publics continueront de recevoir chaque année, même après l'entrée en vigueur des modifications des lois de procédure applicables, des milliers de plaintes et autres documents similaires sous format papier, car ces requêtes émanent généralement de particuliers qui ne souhaitent pas s'inscrire au préalable sur la plateforme centralisée. Cette quantité considérable de documents est rédigée spécialement à l'intention des autorités pénales et souvent complétée par des photocopies de documents pertinents sur le plan juridique. Dans les deux cas, la source ou l'original reste chez l'expéditeur.

Si la LPCJ n'est pas interprétée de manière restrictive, ce qui, selon les explications relatives à l'avant-projet actuel, ne devrait pas être le cas, une loi visant à introduire les communications judiciaires électroniques instaurera de nouvelles obligations de renvoi dans le processus papier, qui n'existaient pas encore dans le monde analogique. Cela ne peut pas avoir été la volonté du législateur.

Le renvoi de documents n'a aucune utilité si la finalité d'un document se limite à la transmission du message qu'il contient. Les expéditeurs de ces messages disposent déjà de copies de leurs demandes ou des originaux dont ils ont fait des photocopies. Les exemplaires renvoyés seront donc très majoritairement jetés dès qu'ils seront revenus chez leurs expéditeurs d'origine.

Même dans le cas, plutôt rare, où des divergences surgiraient *a posteriori* quant à savoir si les copies numérisées figurant dans les dossiers administratifs correspondent aux documents déposés, les documents renvoyés ne pourraient pas servir de preuve, car il serait impossible de déterminer si ce sont bien ces documents qui ont été déposés auprès de l'autorité.

La distinction entre les simples communications et les documents qui, outre le contenu de la communication, comportent un contenu supplémentaire, est déjà prévue dans la LPCJ.

L'article 30, alinéa 2 de la LPCJ prévoit que les documents peuvent être conservés par les autorités s'ils sont encore nécessaires dans le cadre de la procédure. Il ressort du message y relatif du 15 février 2023 (FF 2023 679ss) que les documents ayant valeur de titre ne doivent pas être renvoyés immédiatement (commentaires relatifs à l'art. 30 P-LPCJ, p. 35). Cela signifie également que l'obligation de renvoyer les actes officiels, dont la restitution présente un intérêt pour les expéditeurs, n'est pas remise en cause en l'espèce.

En revanche, il n'est pas nécessaire de préciser davantage que l'interprétation de la LPCJ au sens d'un nouvel échange postal sous forme papier entraîne une charge supplémentaire considérable en termes de frais de port et de travail. Une interprétation de la loi qui conduit en fin de compte à ce que des milliers de liasses de vieux papiers doivent être affranchies ne peut être justifiée par l'intention du législateur.

Solution proposée

Pour les raisons susmentionnées, il est proposé en l'espèce d'insérer un nouvel article 22a. La formulation choisie précise que les documents conservés conformément à l'article 30, alinéa 2, de la LPCJ ne sont pas exemptés de l'obligation de renvoi. Si, en revanche, l'un des critères mentionnés ci-après s'applique, il est certain que l'expéditeur ne tire aucune valeur ajoutée d'un renvoi, raison pour laquelle il semble nécessaire, en se référant à l'objectif normatif du législateur, d'inscrire dans l'ordonnance une interprétation restrictive de la notion de document conformément à l'article 30 LPCJ. Si l'expéditeur a un intérêt à ce que le document lui soit renvoyé, il peut en faire la demande au préalable.

Chapitre 2 *Numérisation et renvoi de documents physiques et notification de copies papier de documents originaux générés par voie électronique*

[…]

Art. 22a *Renvoi des documents physiques*

Sauf demande préalable en ce sens de la part de l'expéditeur ou de l'expéditrice, les pièces du dossier sont exemptées de l'obligation de renvoi des documents remis physiquement prévue à l'article 30, alinéa 1, LPCJ, s'ils ne relèvent pas de l'article 30, alinéa 2, LPCJ et s'ils ne doivent pas être signés à la main conformément au droit procédural applicable ou s'ils ont la même valeur probante sous forme numérisée, à savoir les impressions de documents créés électroniquement ou les photocopies.

Art. 22*b* **Notification de copies papier de documents originaux générés par voie électronique (nouveau)**

Problématique :

Comment joindre les personnes qui ne sont pas joignables sur la plateforme ?

Au chiffre 2.6 du rapport explicatif relatif à l'ouverture de la procédure de consultation (p. 7), il est précisé que l'idée de garantir la notification des décisions finales signées électroniquement par l'envoi de copies papier a été écartée, car les dispositions légales applicables ne le permettaient pas. Concrètement, il s'agit du fait que l'article 353, alinéa 1, lettre k du nCPP prescrit, pour l'ordonnance pénale du ministère public : *« L'ordonnance pénale contient les informations suivantes : (…) la signature de la personne qui a établi l'ordonnance, si elle est notifiée sur papier. »* L'article 238, lettre h, du nCPC contient une disposition similaire pour les décisions des tribunaux civils.

L'article 22 concrétise l'article 29 de la LPCJ (numérisation des documents physiques) et donc le passage du support papier au dossier électronique. Le processus inverse n'est toutefois pas décrit dans la LCPJ, bien qu'il s'agisse en pratique d'une exigence très importante, car selon le concept de base de la LPCJ, la création électronique de dossiers doit être la norme. Toutefois, lorsque des particuliers ne souhaitent pas

s'inscrire sur une plateforme de transmission électronique, ils conserveront à l'avenir le droit de se voir remettre un exemplaire papier des communications et des décisions.

En particulier, les autorités pénales chargées des contraventions et les services des ordonnances pénales des ministères publics rendent chaque année des dizaines de milliers de décisions définitives. Si ces procédures sont exclues de la gestion électronique des dossiers, parce que, selon l'interprétation (désormais abandonnée) des dispositions procédurales applicables par l'ordonnance relative à la LPCJ, il faudrait tout de même les traiter sur papier, il ne resterait alors qu'un volume compris entre 10 et 20 % des dossiers pouvant être gérés par voie électronique. C'est notamment dans le domaine des affaires de masse que le potentiel de rationalisation de la digitalisation s'évapore.

Certes, la LPCJ repose sur le principe réglementaire selon lequel les particuliers ne doivent pas être contraints de communiquer par voie électronique avec les autorités, et il ne s'agit donc pas ici de remettre en cause ce principe. En revanche, il ne peut être juste d'interpréter l'exigence de signature de manière si restrictive qu'elle freine tout progrès.

Il ressort de l'article 22, alinéa 2, LPCJ qu'à l'avenir, un cachet électronique réglementé devra garantir qu'un document établi par voie électronique provient bien de l'autorité compétente, telle qu'elle ressort par exemple de l'en-tête ou d'un élément similaire. À propos de cet article, le message relatif à la LPCJ précise : « L'exigence de signature constitue souvent un obstacle à la numérisation. Au lieu de la signature, la loi prévoit l'authentification à l'aide d'un moyen d'identification électronique reconnu ainsi que l'apposition d'un cachet électronique réglementé. » (Message relatif à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 15 février 2023; FF 2023 679ss, remarques préliminaires concernant l'art. 22, p. 30). Il en résulte que le cachet électronique réglementé remplace la signature manuscrite dans le cadre de la gestion électronique des dossiers. Il n'y a donc plus de place pour un recours à l'article 14 CO dans le champ d'application de la LPCJ. La LPCJ, en tant que loi plus récente et plus spécifique, remplace la signature manuscrite des membres des autorités par un cachet électronique réglementé (concernant le niveau de protection, cf. le message, *op. cit.*, ad art. 22 LPCJ).

Solution proposée

Il convient certes de donner raison au rapport explicatif accompagnant l'ouverture de la procédure de consultation sur ce point, dans la mesure où il ressort des lois de procédure applicables que, par exemple, les décisions définitives doivent porter la signature de la personne qui les a rendures lorsqu'elles sont envoyées **sous forme d'original** sur papier. Selon l'avis défendu ici, cette formulation permet toutefois tout à fait une interprétation conforme à l'objectif manifeste et sans équivoque de la loi.

Aujourd'hui déjà, il est d'usage courant auprès des tribunaux civils et des autorités pénales de verser l'original des décisions définitives au dossier de l'autorité et de remettre aux parties une photocopie de l'original. Comme déjà mentionné plus haut concernant la disposition relative au renvoi des documents papier envoyés, c'est en renonçant à une interprétation restrictive qu'une **nouvelle obligation est créée dans le monde analogique**. Si l'on suit le rapport explicatif, il y aurait soudainement une obligation d'envoyer des originaux papier. Cela multiplierait de manière exponentielle l'envoi d'originaux papier dans le monde numérique. Cela ne peut avoir été l'intention du législateur.

En conséquence, il convient de préciser dans l'ordonnance que la notification des documents nécessitant une signature à des personnes qui ne sont pas enregistrées sur la plateforme peut bien sûr continuer à se faire, à l'avenir également, au moyen d'une copie papier de l'original (désormais établi par voie électronique), qui reste dans le dossier numérique. Une copie papier de l'original électronique a exactement la même valeur informative qu'une décision portant une signature manuscrite. Si le destinataire a des doutes quant à l'authenticité de la décision, il peut à tout moment se faire envoyer l'original électronique ou se le faire présenter au siège de l'autorité, ce qui lui permet en outre de vérifier la date de création de l'original indiquée sur la copie papier.

La solution proposée présenterait l'avantage d'éviter qu'il n'y ait, dans une même procédure, deux originaux de la même décision coexistant parallèlement (par exemple lorsqu'une personne accusée est défendue et qu'un exemplaire muni d'un cachet électronique de la décision finale (sans aucune signature) pourrait lui être envoyé par l'intermédiaire de son représentant légal, alors que la partie civile n'est pas représentée par un avocat et qu'il faudrait lui envoyer une copie papier qui, à son tour, devrait porter une signature manuscrite). En outre, cela créerait une situation juridique identique à celle de la juridiction fédérale. La LPCJ n'exige justement pas que les jugements portent une signature lorsqu'ils sont envoyés sur papier.

Pour les raisons exposées au point 3.1, il est donc proposé d'insérer un nouvel article 22b:

> ***Art. 22b*** *Notification de copies papier de documents générés par voie électronique*
>
> *Les autorités qui gèrent leurs dossiers par voie électronique apposent un cachet électronique réglementé sur les documents pour lesquels le droit procédural applicable prévoit, pour leur forme papier, la signature d'au moins un représentant de l'autorité, lorsqu'elles doivent envoyer ces documents. Dans la mesure où de tels documents doivent (également) être notifiés à des personnes avec lesquelles l'autorité ne communique pas par voie électronique, la transmission du document s'effectue au moyen d'une copie papier de l'original électronique. La notification de la copie papier fait courir le délai si les personnes destinataires sont informées sur la copie papier qu'elles peuvent obtenir gratuitement l'original électronique via une plateforme conformément à la LPCJ ou demander à l'autorité un double signé à la main.*

Si l'on s'en tient à l'interprétation beaucoup trop restrictive de la LPCJ, telle qu'elle est esquissée dans les explications relatives au projet de l'OCEP, il faudrait au moins envisager l'utilisation d'une signature électronique qualifiée des membres de l'autorité (en plus du cachet de l'autorité) afin de satisfaire à la notion de « signature » utilisée dans les lois de procédure, bien que celle-ci, comme indiqué plus haut, ait été remplacée par le cachet de l'autorité dans le contexte de la gestion numérique des dossiers.

Chapitre 3: Transmission de documents par un autre moyen qu'une plateforme au sens de la LPCJ

Section 1 Recours à d'autres solutions pour la transmission de documents

Art. 23 Exigences

On ne sait pas exactement comment l'Office fédéral de la justice délimite le champ d'application matériel et pratique de l'art. 23 par rapport à l'art. 24 de l'OCEP. Des exemples concrets manquent.

Cette disposition concrétise l'article 128b, alinéa 2, du Code de procédure civile (CPC), l'article 103b, alinéa 2, du Code de procédure pénale (CPP) et l'article 8c, alinéa 2, de la loi sur l'aide aux victimes du 23 mars 2007 (LAVI). Nous partons du principe que cette disposition vise la communication entre les autorités pénales au sein de la chaîne de procédure pénale, dans le cadre de laquelle les dossiers doivent par exemple être transmis à l'instance supérieure en cas de recours, lorsque d'autres autorités sont chargées de certains actes de procédure (ex. mandat d'enquête du ministère public à la police judiciaire) ou lors de la transmission des résultats d'actes d'enquête que la police transmet au ministère public.

Un deuxième champ d'application est la chaîne de procédure civile, par exemple lorsqu'un tribunal civil ordonne à l'office des poursuites, à l'office des faillites ou à l'office du registre du commerce d'accomplir un acte déterminé ou lorsque le tribunal de première instance transmet ses dossiers à l'instance cantonale supérieure en raison d'un recours.

La transmission physique des dossiers entre les autorités pénales s'effectue actuellement encore souvent par la poste, par courrier interne ou par coursier. La mission confiée à la police pour une mesure d'instruction est généralement formulée par écrit, mais ni la date exacte ni la réception ne sont consignées séparément.

Les dispositions d'exécution proposées s'inspirent fortement de la solution technique de la plateforme. Pour la transmission électronique au sein du canton (CPC) ou entre autorités pénales (CPP), il faudrait toutefois appliquer d'autres exigences que pour la communication via la plateforme.

La transmission électronique au sein d'un canton pourra par exemple s'effectuer à l'avenir par la modification des droits d'accès à la base de données cantonale commune. Pour cela, nous estimons qu'aucune quittance n'est nécessaire. L'enregistrement dans les fichiers de journalisation (logfiles) du système informatique cantonal suffit. Du point de vue de la protection des données et de la sécurité informatique, la modification des droits d'accès est clairement préférable à l'envoi répété de documents via une plateforme externe.

L'article 23 devrait être complété de manière à autoriser la transmission électronique de documents par la modification des droits d'accès à une base de données commune. La traçabilité des moments de la transmission ou des moments de la modification des droits d'accès doit être garantie. Les exigences du CPC et du CPP ne vont pas jusqu'à rendre nécessaire, dans le cadre du passage au numérique, un horodatage synchronisé comme celui prévu à la lettre b. Il convient donc de renoncer à ce critère.

Art. 24 Transmission par voie électronique entre les autorités

L'intitulé est trop général et donc trompeur. Il s'agit toujours de communications émanant des autorités pénales ou destinées à celles-ci, ou des tribunaux civils, ou à destination de ceux-ci, dans le cadre de procédures relevant du CPP ou du CPC. Parallèlement, il semble nécessaire de définir la notion des autres autorités, c'est-à-dire celles qui sont soumises à l'obligation de communiquer par voie électronique avec les autorités pénales (cf. la consultation relative à l'art. 6 OECP). Une incertitude subsiste à cet égard, notamment en ce qui concerne les corporations de droit public qui n'agissent pas dans l'exercice de la puissance publique.

Cette disposition précise les exceptions prévues à l'article 128c, alinéa 2, CPC, à l'article 103c, alinéa 2, CPP et à l'article 8d, alinéa 2, de la LAVI. Ces exceptions sont justifiées lorsque, dans le cadre de procédures civiles ou pénales, un grand nombre de communications avec les autorités sont nécessaires, communications qui ne font pas partie de la chaîne de procédure pénale ou civile, et lorsque la communication directe, par exemple via une interface, est préférable aux communications électroniques dans le domaine judiciaire via la plateforme, notamment pour la transmission de métadonnées ou pour des raisons de coût. Dans le cadre de la procédure pénale, on peut penser par exemple aux autorités fiscales ou de migration, ou encore aux grandes entreprises de transport ou aux instituts de médecine légale, qui devraient également relever de la notion d'autorité. Il en va de même pour certaines autorités fédérales telles que l'OFDF.

Les conditions devraient s'inspirer de l'article 23 et ne pas aller au-delà. En tout état de cause, on ne voit pas pourquoi l'article 24 prévoit des exigences plus strictes, étant donné que l'article 103c, alinéa 2, CPP – contrairement à l'art. 103b, alinéa 2, CPP, qui prévoit l'enregistrement du moment de transmission et la protection du dossier contre toute modification et toute consultation non autorisée – n'impose aucune exigence quant à la documentation d'une transmission.

Section 2: Transmission de documents par voie électronique dans le domaine de la poursuite pour dettes et la faillite

Art. 25

Aucune remarque.

Section 3: Attestation par voie électronique de l'exactitude du procès-verbal en procédure pénale et en procédure pénale militaire

Art. 26

Aucune remarque.

Chapitre 4: Dispositions finales

Art. 27 Abrogation et modification d'autres actes

Aucune remarque.

Art. 28 Entrée en vigueur

Le financement du projet Justitia 4.0, qui met en place la plateforme centralisée pour le compte des cantons, de la Confédération et des autorités judiciaires, est assuré jusqu'à fin 2027. Le financement de la plateforme centralisée pourrait déjà se faire par des émoluments à partir du 1er juillet 2027 mais au plus tard au 1er janvier 2028. L'ordonnance devrait donc entrer en vigueur en même temps que l'entrée en vigueur finale de la loi.

Si d'autres articles de la LPCJ devaient être mis en vigueur par anticipation en vue de l'octroi de l'autorisation d'exploitation (voir nos commentaires relatifs à l'article 3), il faudrait procéder de la même manière pour les dispositions correspondantes de l'ordonnance (section 2).

Abrogation et modification d'autres actes

Abrogation OCEI-PA

Aucune remarque.

Abrogation OCEI-PCPP

Nous avons pris connaissance de la note de service du 29 avril 2026 et nous sommes favorables à ce que les dispositions transitoires permettent aux cantons de continuer à utiliser les plateformes de notification autorisées jusqu'à présent.

Nous voyons d'un œil critique le fait que les autorités judiciaires soient contraintes, dans le cadre des procédures relevant du code de procédure civile (CPC) et du code de procédure pénale (CPP), d'utiliser et de gérer en parallèle deux systèmes de communication pendant une période transitoire de plusieurs années, avec éventuellement des exigences formelles différentes (signature électronique qualifiée). Les dispositions transitoires devraient être harmonisées de manière à ce que les procédures déjà en cours puissent être menées selon le nouveau droit via la plateforme. Nous invitons l'Office fédéral de la justice à rechercher, en collaboration avec les autorités judiciaires et Justitia 4.0, une solution satisfaisante pour toutes les parties.

Art. 14a OSCSE Signatures et cachets électroniques vérifiés par le validateur

Aucune remarque.

Art. 14b OSCSE Apposition et validation de signatures et de cachets électroniques

Aucune remarque.

Kantonsgericht Kollegiumstrasse 28
Postfach 2265
6431 Schwyz
Telefon 041 819 26 55

kantonschwyz

per E-Mail

KAN 2026 4

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Dossier: **KAN 2026 4**
betreffend: Vernehmlassungen
Datum: 22. Juni 2026 pne

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Am 13. März 2026 haben Sie die Kantone eingeladen, zum Vorentwurf des EJPD betreffend die Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung zu nehmen. Das Kantonsgericht Schwyz nimmt diese Gelegenheit hiermit gerne wahr.

Die Vorlage wird in ihrer Zielsetzung grundsätzlich begrüsst. Sie bildet eine wichtige Grundlage für die Umsetzung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) und für die künftige elektronische Kommunikation in Justizverfahren. Zu den nachfolgenden Punkten erlauben wir uns Bemerkungen:

Ingress

Im Ingress sollten sämtliche relevanten Delegationsnormen aufgenommen werden. Dies erscheint insbesondere dort angezeigt, wo die Verordnung technische oder formelle Anforderungen konkretisiert, die sich aus den verschiedenen Verfahrensgesetzen ergeben. Eine möglichst vollständige Abbildung der gesetzlichen Grundlagen erhöht die Klarheit und Nachvollziehbarkeit der Verordnung.

Art. 2 Anforderungen an die Plattformen

Die Anforderungen an die Plattformen erscheinen grundsätzlich sachgerecht.

Die in Art. 2 Abs. 1 Bst. c vorgesehene maximale Dokumentengrösse von zwei Gigabyte hängt jedoch stark von der technischen Entwicklung ab. Angesichts stetig steigender Dateigrössen erscheint eine Erhöhung in naher Zukunft unabdingbar, weshalb sich die Frage stellt, ob der Grenzwert nicht höher anzusetzen ist.

Unklar erscheint zudem die Löschfunktion nach Art. 2 Abs. 1 lit. d. Aus dem Wortlaut geht nicht eindeutig hervor, ob tatsächlich das Dokument selbst gelöscht wird oder lediglich die Berechtigung bzw. Sichtbarkeit im Benutzerprofil entfällt. Ebenfalls nicht hinreichend klar ist, ob und inwiefern zwischen Behörden und übrigen Nutzerinnen und Nutzern unterschieden wird. Dies sollte präzisiert werden.

Art. 4 Format der Dokumente

Die Vorgabe, wonach Behörden ihre Dokumente im Format PDF/A übermitteln, wird begrüsst. PDF/A ist für die Archivierung und die einheitliche Weiterverarbeitung elektronischer Akten grundsätzlich geeignet.

Kritisch erscheint hingegen die weitgehende Formatfreiheit bei Beilagen. In der Praxis dürfte es für eine effiziente und sichere Aktenbearbeitung sinnvoll sein, Beilagen im Regelfall im Format PDF einzureichen. Eine Übermittlung im Originalformat sollte vor allem dann vorgesehen werden, wenn PDF ungeeignet ist, den Inhalt des Dokuments korrekt wiederzugeben, oder wenn Primärdaten erforderlich sind.

Art. 5 Quittungen

Art. 5 Abs. 2 Bst. d Ziff. 2 enthält einen Widerspruch. Eine Quittung bezieht sich auf übermittelte Dokumente. Dokumente, die aufgrund der Virenprüfung oder aus anderen Gründen nicht übermittelt wurden, können daher nicht Bestandteil einer Eingangsquittung sein. Bei Nichtübermittlung sollte die Plattform der Absenderin oder dem Absender vielmehr eine entsprechende Meldung zustellen.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Art. 6 sollte dahingehend präzisiert werden, dass die Bestimmung nur verfahrensleitende Behörden betrifft, die über ein entsprechendes Behördenprofil auf der Plattform verfügen. Es sollte vermieden werden, dass sämtliche Behörden, die in irgendeiner Form an Verfahren beteiligt sein können, als siegelungspflichtig verstanden werden. Eine solche Auslegung könnte erhebliche organisatorische und finanzielle Auswirkungen haben und würde den Anwendungsbereich der Plattform unnötig ausweiten.

Art. 9 Profile

Der Mehrwert der Postadresse in den Profilen erscheint fraglich. Bei Behörden können mehrere Standorte oder Zustelladressen bestehen. Bei natürlichen Personen und Organisationen ist zudem nicht ohne Weiteres gewährleistet, dass die hinterlegte Postadresse aktuell und verlässlich ist. Es sollte deshalb geprüft werden, ob auf die Postadresse als zwingende Profilangabe verzichtet werden kann.

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Es wird grundsätzlich begrüsst, dass die Plattform nicht als Langzeitablage ausgestaltet wird. Die automatische Löschung von Dokumenten nach einer gewissen Zeitspanne ist sachgerecht, weil die massgebenden Akten in den Geschäftsverwaltungs- bzw. Fachsystemen der Behörden geführt werden müssen.

Für Quittungen erscheint eine Aufbewahrungsfrist von sechs Monaten jedoch zu kurz. Quittungen können auch zu einem späteren Zeitpunkt im Verfahren erforderlich sein, insbesondere zum Nachweis der Fristwahrung, der Übermittlung oder des erstmaligen Abrufs. Für Quittungen sollte deshalb eine längere Aufbewahrungsfrist vorgesehen werden. Vorgeschlagen wird eine Frist von drei Jahren nur für Quittungen.

Art. 14 Virenprüfung

Grundsätzlich ist anzustreben, dass die Virenprüfung möglichst vollständig durch die Plattform erfolgt. Eine starre Dateigrössengrenze sollte daher nicht in der Verordnung festgelegt werden. Einerseits ist davon auszugehen, dass sich die technischen Möglichkeiten zur Prüfung grösserer Dateien in naher Zukunft weiterentwickeln werden. Andererseits kann die Bekanntgabe einer fixen Grenze potenziellen Angreifern Hinweise darauf geben, wie Schadsoftware in grossen Dateien platziert werden könnte, um eine Erkennung zu erschweren.

Gleichzeitig muss die Übermittlung von Dateien auch dann möglich bleiben, wenn keine oder nur eine eingeschränkte Virenprüfung durchgeführt werden kann. Dies betrifft insbesondere grosse Datenbestände, verschlüsselte oder passwortgeschützte Dateien sowie forensische Daten, wie sie namentlich in Strafverfahren vorkommen können. Solche Daten müssen in der Praxis sicher übermittelt werden können; andernfalls besteht die Gefahr, dass auf weniger geeignete oder unsichere Ausweichkanäle zurückgegriffen wird.

In diesen Fällen ist eine klare und verständliche Kennzeichnung wesentlich. Die Empfängerin oder der Empfänger muss ohne Weiteres erkennen können, ob keine oder nur eine eingeschränkte Virenprüfung erfolgt ist, damit sie oder er vor der weiteren Bearbeitung lokal eine vollständige Virenprüfung durchführen kann. Die Plattform sollte die Beteiligten entsprechend deutlich darauf hinweisen.

Schliesslich ist klarzustellen, dass bei nicht übermittelten Dateien keine Quittung ausgestellt wird. In solchen Fällen soll die Plattform der Absenderin oder dem Absender lediglich eine entsprechende Mitteilung über die Nichtübermittlung zustellen.

Art. 22 Digitalisierung von physischen Dokumenten

Die Vorgaben zur Digitalisierung physischer Dokumente werden grundsätzlich begrüsst.

Hinsichtlich der Rücksendung physisch eingereichter Dokumente erscheint es nicht sachgerecht, durch die Einführung der elektronischen Aktenführung neue Rücksendungspflichten für Papierdokumente zu schaffen, die in der bisherigen analogen Praxis nicht bestanden. Dies betrifft insbesondere physisch eingereichte Eingaben, deren Zweck sich in der Mitteilung an die Behörde erschöpft, sowie Kopien von Dokumenten, deren Originale bei der Absenderin oder beim Absender verbleiben.

Es sollte deshalb eine Regelung aufgenommen werden, wonach physisch eingereichte Aktenstücke ohne vorgängiges anderslautendes Ersuchen der Absenderin oder des Absenders nicht zurückgesendet werden müssen, sofern sie nicht nach Art. 30 Abs. 2 BEKJ zurückzubehalten sind und ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich bei Ausdrucken elektronisch erstellter Dokumente oder Fotokopien.

Ergänzend sollte die Verordnung klarstellen, wie mit Dokumenten umzugehen ist, die von der Behörde elektronisch erstellt und gesiegelt werden, aber Personen zugestellt werden müssen, die nicht über die Plattform erreichbar sind. Die elektronische Aktenführung darf nicht dadurch entwertet werden, dass für solche Zustellungen wieder ein handschriftlich unterzeichnetes Papieroriginal erstellt werden muss. Gerade in Verfahren mit hohen Fallzahlen würde dies erhebliche Medienbrüche verursachen und den mit der Digitalisierung angestrebten Effizienzgewinn weitgehend relativieren. Sachgerecht erscheint deshalb, dass in solchen Fällen eine Papierkopie des elektronisch gesiegelten Originals zugestellt

werden kann. Zur Wahrung der Rechtssicherheit kann vorgesehen werden, dass die empfangende Person bei Bedarf Zugang zum elektronischen Original erhält oder ein handschriftlich unterzeichnetes Doppel verlangen kann.

Art. 23 Eignungsvoraussetzungen

Die vorgeschlagene Regelung erscheint zu stark an der Funktionsweise der BEKJ-Plattformen orientiert. Sie berücksichtigt nicht ausreichend, dass die elektronische Weitergabe von Akten innerhalb eines Kantons oder innerhalb einer Verfahrenskette auch durch Mutation von Zugriffsrechten auf einer gemeinsamen Datenbank oder durch vergleichbare technische Lösungen erfolgen kann.

In solchen Konstellationen braucht es nicht zwingend eine Quittung. Eine nachvollziehbare Protokollierung in den Logfiles des kantonalen IT-Systems kann genügen, sofern ersichtlich ist, wann der Zugriff eingeräumt oder verändert wurde. Die Bestimmung sollte entsprechend offener formuliert werden.

Art. 24 Elektronische Übermittlung unter Behörden

Die Sachüberschrift und der Wortlaut von Art. 24 erscheinen zu weit gefasst. Die Bestimmung sollte klarer auf die Kommunikation von und zu Strafbehörden oder Zivilgerichten im Rahmen der einschlägigen Verfahren ausgerichtet werden. Es sollte vermieden werden, dass die Bestimmung als allgemeine Regelung für beliebige Behördenkommunikation verstanden wird.

Zudem sollte der Begriff der übrigen Behörden präzisiert werden. Unklarheiten bestehen insbesondere bei öffentlich-rechtlichen Körperschaften oder Stellen, die nicht hoheitlich handeln. Die Anforderungen an alternative technische Lösungen sollten sich an Art. 23 orientieren und nicht darüber hinausgehen, soweit die massgebenden Verfahrensgesetze keine weitergehenden Anforderungen vorsehen.

Art. 28 Inkrafttreten

Die VEKJ sollte gleichzeitig mit der abschliessenden Inkraftsetzung des BEKJ in Kraft treten. Nur so ist gewährleistet, dass die für die operative Umsetzung notwendigen Ausführungsbestimmungen rechtzeitig und kohärent zur Verfügung stehen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüssen
Patrick Neidhart, für das Kantonsgericht

i.V.

Empfänger: - Eidgenössisches Justiz- und Polizeidepartement (EJPD), Bern

KKLJV CCSPC CDSPC

Herr Bundesrat Beat Jans
Vorsteher Eidgenössisches Justiz- und Polizeidepartement
EJPD

übermittelt per E-Mail an cornelia.perler@bj.admin.ch

Bern, 22. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ); Stellungnahme KKLJV

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie verschiedene Adressaten zur Vernehmlassung in titelerwähnter Sache eingeladen. Die Konferenz der kantonalen Leitenden Justizvollzug KKLJV erlaubt sich als Fachkonferenz der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) für den Justizvollzug ebenfalls Stellung zu nehmen.

Der Justizvollzug, als eine kantonale Aufgabe, stellt eine wichtige Säule des Strafjustizsystems dar. Es bestehen zahlreiche Schnittstellen zu den Strafbehörden, dies bereits schon während des Strafverfahrens wie auch nach dessen Abschluss (u.a. auch im Zusammenhang mit den gerichtlichen Nachverfahren). Im Gegensatz zur Strafprozessordnung ist das Vollzugsrecht jedoch kantonal geregelt. Der Justizvollzug zeichnet sich ausserdem durch eine stark interkantonal geprägte Zusammenarbeit aus. Die mit BEKJ verfolgten Ziele der durchgängig digitalen und medienbruchfreien Verfahren können jedoch nur erreicht werden, wenn die Justizvollzugsbehörden als wichtige Teilnehmerinnen der Strafprozesskette (chaîne pénale) auch für die Verwaltungsverfahren dasselbe System nutzen können. Dies ist insbesondere von grosser Bedeutung im Hinblick auf die Einführung einer interkantonalen elektronischen Justizvollzugsakte (eJVAkte).

Aus diesem Grund beantragen wir, in der VEKJ auch spezifische Bestimmungen vorzusehen, welche die Nutzung der Plattform für kantonale Verwaltungsverfahren des

Justizvollzugs ermöglichen. Entsprechend ist bei Art. 1 Abs. 1 analog lit. c (Verwaltungsverfahren des Bundes) eine lit. d einzuführen:

d *interkantonale Plattform für den Justizvollzug.*

Die Kantone werden gemäss Art. 16 VEKJ 90 Prozent der Gebühren der zentralen Plattform tragen. Der Einbezug der kantonalen Verwaltungsverfahren des Justizvollzugs erhöht den Nutzen für die Kantone und trägt zur wirtschaftlichen Rechtfertigung des Systems bei.

Im Weiteren verweisen wir auf die detaillierteren Ausführungen betr. Einbezug der verwaltungsrechtlichen Verfahren des Justizvollzugs in der Stellungnahme von HIS Schweiz.

Wir bedanken uns bei Ihnen, sehr geehrter Herr Bundesrat, für die Entgegennahme unserer Stellungnahme und die Berücksichtigung unserer Anliegen.

Mit hochachtungsvollen Grüssen

Romilda Stämpfli
Präsidentin KKLJV

Katja Schnyder-Walser
Geschäftsführerin KKLJV

KKPKS CCPCS
Konferenz der kantonalen Polizeikommandantinnen und -kommandanten
Conférence des commandantes et des commandants des polices cantonales
Conferenza delle e dei comandanti delle polizie cantonali

Der Präsident

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrat Beat Jans
Bundeshaus West
3003 Bern

Per E-Mail an:
cornelia.perler@bj.admin.ch

Bern, 5. Juni 2026

Stellungnahme der KKPKS zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Die Konferenz der kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) bedankt sich für die Möglichkeit, zu oben genannter Vernehmlassung Stellung nehmen zu können.

Aus polizeilicher Sicht ist im Rahmen dieser Vorlage von zentraler Bedeutung, dass die behördeninterne Kommunikation primär zwischen den kantonalen Polizeikorps und den kantonalen Staatsanwaltschaften durch die Implementierung der vorgesehenen Plattform gemäss BEKJ in keiner Weise beeinträchtigt wird. Dies ist insbesondere bei der Festlegung des Anwendungsbereichs von Art. 23 und 24 VE-VEKJ zu berücksichtigen.

Bei der konkreten technischen Umsetzung der Vorlage, gilt es, sofern die Einlieferung von Dokumenten sowie der Empfang von Quittungen künftig direkt in den Vorgangsbearbeitungssystemen der Polizei erfolgt, aus Sicht der KKPKS sodann zu bedenken, dass gegebenenfalls auch die für die entsprechenden Schnittstellen anzuwendenden eCH-Standards spezifiziert werden müssen. Diesbezüglich könnte beispielsweise eine Orientierung am interkantonal im Polizei- und Justizumfeld angewendeten Standard eCH0051 zielführend sein. Die entsprechenden technischen Spezifikationen sind jedoch nicht auf Verordnungsstufe zu regeln. Nichtsdestotrotz ist auch im Hinblick auf die Schnittstellen zu verhindern, dass die behördeninterne Kommunikation im Rahmen der Implementierung der Vorlage beeinträchtigt wird und allenfalls ist die Aufnahme eines entsprechenden Hinweises im erläuternden Bericht angezeigt.

Zudem gilt es im Hinblick auf technische Spezifikationen zwingend die zeitliche Dynamik sowie die rasante Entwicklungsgeschwindigkeit im Bereich der Informatik zu berücksichtigen. Da insbesondere auch die kantonalen Staatsanwaltschaften und Gerichte von der Vorlage betroffen sind, verweisen wir darüber hinaus ausdrücklich auf die umfassende und detaillierte

Der Präsident

Stellungnahme der Schweizerischen Staatsanwaltschaftskonferenz (SSK). Den diesbezüglichen Ausführungen kann sich die KKPKS vollumfänglich anschliessen.

Besten Dank für Ihre Kenntnisnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Der Präsident

_____
Matteo Cocchi, Kdt Kantonspolizei Tessin

Kopie: Mitglieder der KKPKS, GS KKJPD, GS SSK

OBERGERICHT
DES KANTONS SCHAFFHAUSEN
Frauengasse 17 8200 Schaffhausen 052 632 74 22 justiz.sh.ch

Per E-Mail an
cornelia.perler@bj.admin.ch

Eidgenössisches Justiz-
und Polizeidepartement EJPD
3003 Bern

Schaffhausen, 28. Mai 2026

Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Am 13. März 2026 haben Sie uns Gelegenheit eingeräumt, zum Vorentwurf des EJPD betreffend die Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung zu nehmen. Das Obergericht des Kantons Schaffhausen lässt sich gerne wie folgt dazu vernehmen:

Intertemporales Recht und IncaMail/PrivaSphere Secure Messaging

Im Erläuternden Bericht wird die Auffassung vertreten, dass in Verfahren, die beim abschliessenden Inkrafttreten des BEKJ bereits hängig waren, die bisherigen anerkannten Zustellplattformen (PrivaSphere Secure Messaging und IncaMail) weiterhin benutzt werden könnten. Die Prozessgesetze würden entsprechende Übergangsbestimmungen enthalten, wonach bei hängigen Verfahren das bisherige Recht anwendbar bleibe (Erläuternder Bericht, S. 8).

Diese Auffassung würde dazu führen, dass die Gerichte und Staatsanwaltschaften noch über viele Jahre hinweg gewährleisten müssten, dass sie neben einer Schnittstelle zur Plattform Justitia.Swiss auch noch andere elektronische Eingaben via PrivaSphere Secure Messaging und IncaMail entgegennehmen und in die elektronische Akte verschieben könnten, und sie dabei jeweils auch prüfen müssten, ob die Eingabe überhaupt noch auf diesem Weg zulässig ist. Die Parteien müssten je nach Verfahren einen unterschiedlichen elektronischen Zustellweg (Plattform oder bisherige Anbieter) wählen und dabei unterschiedliche Formerfordernisse beachten (insbesondere Einfügen einer qualifizierten elektronischen Signatur in "altrechtlichen" Verfahren). Auch die Gerichte müssten für allfällige elektronische Zustellungen in "altrechtlichen" Verfahren spezielle Abläufe vorsehen.

Mit einer solchen Rechtslage wäre weder den Behörden noch der Anwaltschaft gedient. Unseres Erachtens ist aber die im Erläuternden Bericht geäusserte intertemporalrechtliche Einschätzung zur Anwendbarkeit der bisherigen verfahrensrechtlichen Bestimmungen ohnehin unzutreffend, jedenfalls hinsichtlich der von den kantonalen Gerichten anzuwendenden eidgenössischen Prozessordnungen StPO und ZPO. Vielmehr hat unseres Erachtens auch in Verfahren nach StPO und ZPO, welche zum Zeitpunkt des Inkrafttretens des BEKJ bereits hängig waren, die elektronische Kommunikation einzig noch über den Weg der Plattform "Justitia.Swiss" zu erfolgen. Dies aus den folgenden Gründen:

Hinsichtlich verfahrensrechtlicher Übergangsregelungen gilt der **allgemeine intertemporalrechtliche Grundsatz der unmittelbaren Anwendbarkeit neuer verfahrensrechtlicher Regelungen** (vgl. etwa BGE 144 II 273 E. 2.2.4; 129 V 113 E. 2.2; Fridolin Walther, in: Aebi-Müller/Müller [Hrsg.], Berner Kommentar, Schweizerische Zivilprozessordnung, Band III, Bern 2025, Art. 407f N. 6). Neue Verfahrensbestimmungen gelangen mithin grundsätzlich mit ihrem Inkrafttreten auch auf bereits hängige Verfahren zur Anwendung. Der Gesetzgeber kann von diesem Grundsatz abweichen, was er insbesondere beim Inkrafttreten der ZPO und StPO per 1. Januar 2011 Gebrauch tat, da die Anwendung einer grundlegend neuen Verfahrensordnung auf hängige Verfahren zu praktischen Problemen geführt hätte (vgl. Art. 404 ZPO und Art. 450 StPO, letzteres allerdings als Ausnahme zu Art. 448 StPO). Demgegenüber gilt bei der blossen Änderung einzelner Bestimmungen der StPO und der ZPO das neue Recht in der Regel auch für bereits hängige Verfahren (zur *ZPO* vgl. Walther, Art. 407f N. 10; Benedikt Seiler, in: Sutter-Somm et al. [Hrsg.], Kommentar zur Schweizerischen Zivilprozessordnung [ZPO], 4. A., Zürich/Genf 2025, Art. 404 N. 7; Ivo Schwander, in: Brunner/Schwander/Fischer [Hrsg.], Schweizerische Zivilprozessordnung [ZPO], Kommentar, 3. A., Zürich/St. Gallen 2025, Art. 404 N. 20 und 25; zur *StPO* vgl. z.B. BGE 151 IV 84 E. 2.2; BGer 7B_423/2024 vom 12. Juni 2024 E. 4; 6B_563/2022 vom 29. September 2022 E. 1.2.3; vgl. auch Moritz Oehen, in: Niggli/Heer/Wiprächtiger [Hrsg.], Basler Kommentar, Schweizerische Strafprozessordnung/Jugendstrafprozessordnung,

3. A., Basel 2023, Art. 448 N. 2). Bei den Änderungen mit dem BEKJ wurden einzig hinsichtlich der Obligatorien betreffend elektronische Aktenführung und elektronischen Rechtsverkehr übergangsrechtliche Sonderbestimmungen eingeführt (Art. 407g zu Art. 128b und Art. 128c ZPO; Art. 456b zu Art. 100 Abs. 3, Art. 103b und Art. 103c StPO). Die weiteren mit dem BEKJ geänderten oder eingeführten Bestimmungen der StPO und ZPO gelangen daher unmittelbar mit ihrem Inkrafttreten (d.h. voraussichtlich per 1. Juli 2027) auf alle Verfahren zur Anwendung, mithin insbesondere auch auf Verfahren, die in diesem Zeitpunkt bereits rechtshängig sind. Dies entspricht im Übrigen auch der zusätzlichen allgemeinen Übergangsbestimmung von Art. 37 Abs. 1 Satz 3 BEKJ, wonach Benutzerinnen und Benutzer ab dem abschliessenden Inkrafttreten des BEKJ Eingaben über die Plattform einreichen können.

Dies bedeutet unseres Erachtens, dass im Zeitpunkt des abschliessenden Inkrafttretens des BEKJ per 1. Juli 2027 die bisherigen Prozessbestimmungen zum elektronischen Rechtsverkehr (insbesondere Art. 130 Abs. 2 ZPO und Art. 110 Abs. 2 StPO sowie die u.a. darauf gestützte VeÜ-ZSSV) in Verfahren nach der StPO und ZPO nicht mehr zur Anwendung gelangen, und zwar auch nicht auf Verfahren, welche in diesem Zeitpunkt bereits rechtshängig waren. Unseres Erachtens ist daher entgegen der im Bericht vertretenen Ansicht **per 1. Juli 2027 die elektronische Kommunikation in allen Verfahren nach StPO und ZPO nur noch über eine Plattform nach dem BEKJ und nicht mehr über IncaMail oder PrivaSphere Secure Messaging zulässig**.

Selbst wenn aber das Übergangsrecht so gelten sollte, wie es im Erläuternden Bericht festgehalten wird, würde eine solche Interpretation voraussetzen, dass der Bundesrat auch nach Inkrafttreten des BEKJ weiterhin eine Liste der anerkannten Zustellplattformen führen müsste, obwohl in diesem Zeitpunkt die VeÜ-ZSSV nicht mehr in Kraft stehen wird (vgl. Aufhebungsbestimmungen des VE-VEKJ). Denn zweifellos muss bei Zustellungen über die bisherigen Zustellplattformen zu jedem Zeitpunkt vorausgesetzt werden, dass diese weiterhin anerkannt sind, damit sichergestellt ist, dass die Anforderungen von Art. 2 VeÜ-ZSSV erfüllt sind (vgl. auch Art. 3 Abs. 2 VeÜ-ZSSV). Eine nur in der Vergangenheit zurückliegende Anerkennung kann nicht ausreichen. Es ist daher auch aus diesem Grund nicht davon auszugehen, dass nach dem abschliessenden Inkrafttreten des BEKJ bzw. der Aufhebung der VeÜ-ZSSV Zustellungen via PrivaSphere Secure Messaging oder IncaMail tatsächlich weiterhin zulässig sind (vorbehältlich von Art. 6a Abs. 4 VE-VwVG).

Wir regen daher an, den Bericht anzupassen und festzuhalten, dass die elektronische Kommunikation ab Inkrafttreten des BEKJ nur noch über die Plattform Justitia.Swiss und nicht mehr über die bisherigen Plattformen (PrivaSphere Secure Messaging oder IncaMail) erfolgen kann.

Versand in Papierform

Im bisherigen Transformationsprozess zur Digitalisierung hat sich gezeigt, dass insbesondere die starre Unterschriftsregelung in Art. 80 Abs. 2 StPO ein Hindernis für effiziente digitalisierte Abläufe darstellt. Diese Norm schreibt – anders als etwa Art. 133 lit. g und Art. 238 lit. h ZPO – vor, welche Personen bei einem Papierversand die Unterschrift zu leisten haben. Dies verunmöglicht praxistauglichere Lösungen, wie etwa diejenige, welche im Kanton Schaffhausen für Zivil- und Verwaltungsverfahren geschaffen wurde (Unterschrift in Form einer Kanzleibestätigung auf dem Papierausdruck, dass dieser den Inhalt des elektronischen Originals korrekt wiedergibt; vgl. Art. 54a des Justizgesetzes vom 9. November 2009 [JG, SHR 173.200; in Kraft seit 1. Mai 2026]). Zur Veranschaulichung wird auf die Grafik im Anhang verwiesen.

Nichtsdestotrotz teilt das Obergericht die Auffassung des EJPD, dass das BEKJ den Bundesrat nicht ermächtigt, mittels VEKJ Ausnahmen vom Versand in Papierform vorzusehen (vgl. auch Botschaft BEKJ, S. 78 ff., zum Umfang der Delegation an den Bundesrat). Wir regen daher eine möglichst zeitnahe **Anpassung von Art. 80 Abs. 2 StPO durch den Gesetzgeber** an. Die folgende Anpassung von Art. 80 Abs. 2 StPO – analog Art. 238 lit. h ZPO – würde den Kantonen die notwendige Flexibilität gewährleisten. Im gleichen Zug zu prüfen wäre eine entsprechende Anpassung der Unterschriftsregelung zu den Strafbefehlen.

> ***Art. 80 StPO***
>
> *[2] Entscheide ergehen schriftlich; sie werden begründet und den Parteien zugestellt. Erfolgt die Zustellung auf Papier, so werden sie von der Strafbehörde ~~Verfahrensleitung sowie der protokollführenden Person~~ unterzeichnet.*
>
> ***Art. 353 StPO***
>
> *[1] Der Strafbefehl enthält:*
>
> *k. die Unterschrift der Staatsanwaltschaft ~~ausstellenden Person~~, falls der Strafbefehl auf Papier versendet wird.*

Eine solche Anpassung würde auch der Regelung für die elektronische Zustellung entsprechen, welche aufgrund des Behördensiegels ebenfalls keine (elektronische) Signatur der Verfahrensleitung sowie protokollführenden Person bzw. der den Strafbefehl ausstellenden Person vorsieht.

Fehlende Delegationsnormen

Die Delegationsbestimmungen im Ingress des VE-VEKJ scheinen unvollständig zu sein. Es fehlen die Delegationsnormen zum Format der Dokumente (nArt. 21a Abs. 2 und Art. 34 nAbs. 1bis VwVG, nArt. 38e BGG, nArt. 128e nZPO, nArt. 103e StPO sowie die weiteren analogen Bestimmungen in anderen Verfahrensgesetzen).

Art. 4 VE-VEKJ

Die zentrale Plattform scannt alle Dateien auf Viren, dabei kann sie aber grundsätzlich nur ihr bekannte Dateiformate sinnvoll scannen. Aus Sicherheitsgründen sollte unseres Erachtens daher als Grundsatz am standardisierten PDF-Format festgehalten und es sollten nur ausnahmsweise andere Formate zugelassen werden. Im Format PDF kann der Informationsgehalt eines Dokuments in der Regel rechtsgenüglich wiedergegeben werden, nur ausnahmsweise werden andere Formate zwingend benötigt werden (z.B. Audio- oder Videoaufnahmen). Wir schlagen daher folgende abweichende Formulierung von Abs. 2 vor:

> [2] *Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben, kann die Beilage in einem anderen Format übermittelt werden.*

Fraglich scheint, ob das reine Benennen von Formaten in der Verordnung hinreichend ist oder ob weitere technische Details, wie z.B. der Umgang mit passwortgeschützten oder verschlüsselten Dateien, geregelt werden müssen. Dies ist gegebenenfalls in einem Anhang deutlich einfacher zu bewirtschaften als im Haupttext der vorliegenden Verordnung, weshalb wir zudem folgende Fassung von Abs. 3 und 4 vorschlagen:

> [3] *Kann die verfahrensleitende Behörde eine Beilage im Format, in dem sie eingereicht wurde, nicht öffnen, so räumt sie der einreichenden Partei eine angemessene Frist ein, damit diese die Beilage in einem von der Behörde festgelegten Format einreichen kann.*
>
> [4] *Das EJPD regelt die über die Plattformen zu übertragenden Dateiformate.*

Art. 5 VE-VEKJ

Die Eingangsquittung enthält die Liste der übermittelten Dokumente. Die Liste der nicht übermittelten Dokumente sollte deshalb bereits rein sachlogisch nicht in der Eingangsquittung enthalten sein. Zudem sollte die Information über nicht übermittelte Dokumente nicht in der Eingangsquittung "versteckt" sein, sondern separat ausgewiesen werden (s. auch die Bemerkung zu Art. 14 Abs. 5 VE-VEKJ)

Art. 6 VE-VEKJ

Gemäss dem Wortlaut von Art. 6 VE-VEKJ im Vorentwurf reicht es, wenn eine Behörde, die mehrere Dokumente übermittelt, ein Dokument siegelt und mit einem Zeitstempel versieht. Das ist zu begrüssen. In den Erläuterungen steht allerdings: "Bei Versand durch eine Behörde, muss sie *alle* Dokumente mit einem Siegel und einem Zeitstempel versehen" (Hervorhebung hinzugefügt). Dies stellt aus unserer Sicht einen Widerspruch dar.

Im Übrigen ist fraglich, ob eine Rechtsgrundlage für den Erlass der Verordnungsbestimmungen gemäss Art. 6 (und Art. 7) VE-VEKJ durch den Bundesrat besteht (vgl. namentlich Art. 22 BEKJ, wonach der Bundesrat in diesem Kontext [nur] die Form und den Inhalt der

Quittungen sowie die maximale Aufbewahrungsfrist der Dokumente und Quittungen regelt). Das Obergericht begrüsst den Inhalt der vorgeschlagenen Regelungen dennoch.

Art. 7 VE-VEKJ

Das Anbringen des Siegels durch die Plattformen erfolgt auf der Quittung, nie auf den übermittelten Dokumenten. Abs. 1 sollte daher unabhängig von der Zahl der übermittelten Dokumente formuliert, Abs. 2 ganz gestrichen werden.

> *[1] Werden ~~mehrere~~ Dokumente ~~zusammen~~ übermittelt, so bringt die Plattform dafür in einem separaten Dokument das Siegel und den Zeitstempel an. Das Dokument muss die Bezeichnungen aller übermittelten Dokumente, deren Grösse und die dazugehörigen Hashwerte enthalten.*
>
> *~~[2] Dokumente, die bereits über ein Siegel oder eine qualifizierte elektronische Signatur mit einem Zeitstempel verfügen, müssen nicht erneut mit einem Siegel versehen werden.~~*

Art. 12 VE-VEKJ

In Anlehnung an die Zeitspanne von drei Jahren, innert der bei der Schweizerischen Post im Briefverkehr Nachforschungen möglich sind, sollte auch die Aufbewahrungsfrist für *Quittungen* auf drei Jahre erweitert werden.

Art. 14 Abs. 5 VE-VEKJ

Gemäss Art. 14 Abs. 5 VE-VEKJ informiert die Plattform die Absenderin oder den Absender, wenn ein Dokument beim Verdacht auf einen Virus nicht übermittelt wurde. Dies erscheint aus unserer Sicht sinnvoll.

In den Erläuterungen ist sodann festgehalten, dass die Quittung einen Hinweis auf die nicht übermittelten Dokumente enthalte. Diese Information ergibt unseres Erachtens Sinn. Sie sollte aber nicht in der Eingangsquittung "versteckt" sein (vgl. auch zu Art. 5 VE-VEKJ). Vielmehr sollte die Behörde darüber von der Plattform in einem separaten Dokument ausdrücklich informiert werden. Andernfalls müssten die verfahrensleitenden Behörden stets die Eingangsquittungen auf solche Hinweise prüfen, was wenig praktikabel erscheint.

Art. 22 Abs. 2 VE-VEKJ

Gemäss Art. 22 Abs. 2 VE-VEKJ müssen physisch eingereichte Dokumente im Format PDF/A digitalisiert werden. Es stellt sich die Frage, ob das namentlich für Bilder nicht zu einschränkend ist. Bilder sollten unseres Erachtens, wenn sie z.B. wegen relevanter Details stark vergrössert oder für Analysen einem Gutachter übermittelt werden müssen, zumindest auch in anderen Formaten digitalisiert werden können.

Art. 23 VE-VEKJ

Art. 23 VE-VEKJ bezieht sich auf nArt. 128b Abs. 2 und 3 ZPO, nArt. 103b Abs. 2 und 3 StPO sowie nArt. 8c Abs. 2 und 3 OHG. Diese Bestimmungen regeln die Weitergabe von *Akten* zwischen Behörden (für Parteien dürften diese Bestimmungen demgegenüber nicht anwendbar sein, da hier die separaten Regelungen zur Akteneinsicht zur Anwendung gelangen). Entsprechend sollte im Verordnungstext auch überall von "Akten" die Rede sein, und nicht von "Dokumenten" (vgl. demgegenüber 1. Satz von Art. 23 Abs. 1 VE-VEKJ).

Sodann stellt sich die Frage, wie ein Schutz vor Veränderung zu übermittelnder Akten technisch sichergestellt werden soll, lassen sich doch schlussendlich alle Dateien verändern und kann eine Akte namentlich auch nicht gesiegelte Dateien enthalten (z.B. Beilagen zu Rechtsschriften). Stattdessen sollte unseres Erachtens verlangt werden, dass allfällige Veränderungen *nachvollziehbar* sind. Hierfür würde sich namentlich wie bei Art. 24 VE-VEKJ anbieten, dass die Namen, die Grösse und die Hashwerte der übermittelten Aktenstücke in einer mit einem Behördensiegel versehenen Datei dokumentiert sein müssen.

Art. 23 sollte ferner so ergänzt werden, damit die elektronische Weitergabe von Dokumenten durch die – nachvollziehbare – Mutation von Zugriffsrechten auf eine gemeinsame Datenbank zulässig ist, ohne dass hierfür eine separate Quittung ausgestellt werden muss.

Schliesslich scheint eine aussagekräftigere Marginalie zu Art. 23 VE-VEKJ zielführender, insbesondere zur Abgrenzung von Art. 23 zu Art. 24 VE-VEKJ (z.B. "Elektronische Weitergabe von Akten unter Behörden").

Art. 24 VE-VEKJ

Art. 24 VE-VEKJ bezieht sich auf nArt. 128c Abs. 1 und 2 ZPO, nArt. 103b Abs. 1 und 2 StPO sowie nArt. 8c Abs. 1 und 2 OHG. Diese Bestimmungen regeln die Übermittlung von Eingaben oder weiteren Dokumenten, wobei Ausnahmen nur zwischen Behörden zulässig sind. Entsprechend erscheint analog zu unseren Ausführungen in Art. 23 VE-VEKJ eine aussagekräftigere Marginalie zielführender (z.B. "Elektronische Übermittlung von Dokumenten unter Behörden").

Zudem regen wir an, anstelle der "unveränderbaren" (s. Ausführungen zu Art. 23 VE-VEKJ) Aufzeichnung zu verlangen, dass die Informationen in einer mit einem Behördensiegel versehenen Datei aufgezeichnet werden. Ohnehin sollten sich die Voraussetzungen zu Art. 24 an denjenigen von Art. 23 VE-VEKJ orientieren.

Art. 26 VE-VEKJ

Hinsichtlich Art. 26 Abs. 4 VE-VEKJ erscheint unklar, was "Siegel und qualifizierte elektronische Signaturen mit einem Zeitstempel, die durch ein elektronisches Gerät im Sinne der

anwendbaren Verfahrensgesetze angebracht werden", genau bedeuten. Insbesondere unklar erscheint uns die Bedeutung der Voraussetzung des Anbringens durch ein elektronisches Gerät bzw. die Erläuterung hierzu, welche das Siegel selber als elektronisches Gerät zu bezeichnen scheint. Da ein Behördensiegel zwangsläufig auf einem elektronischen Gerät (in der Regel einem Computer) angebracht wird, kann unseres Erachtens die Formulierung "die durch ein elektronisches Gerät im Sinne der anwendbaren Verfahrensgesetze angebracht werden" ersatzlos gestrichen werden.

Sodann erscheint uns unklar, weshalb hier qualifizierte elektronische Signaturen überhaupt erwähnt werden. Mit dem Inkrafttreten des BEKJ sind in den gerichtlichen Verfahren keine qualifizierten elektronische Signaturen mehr vorgesehen. Entsprechend reicht unseres Erachtens auch die Erwähnung des Behördensiegels.

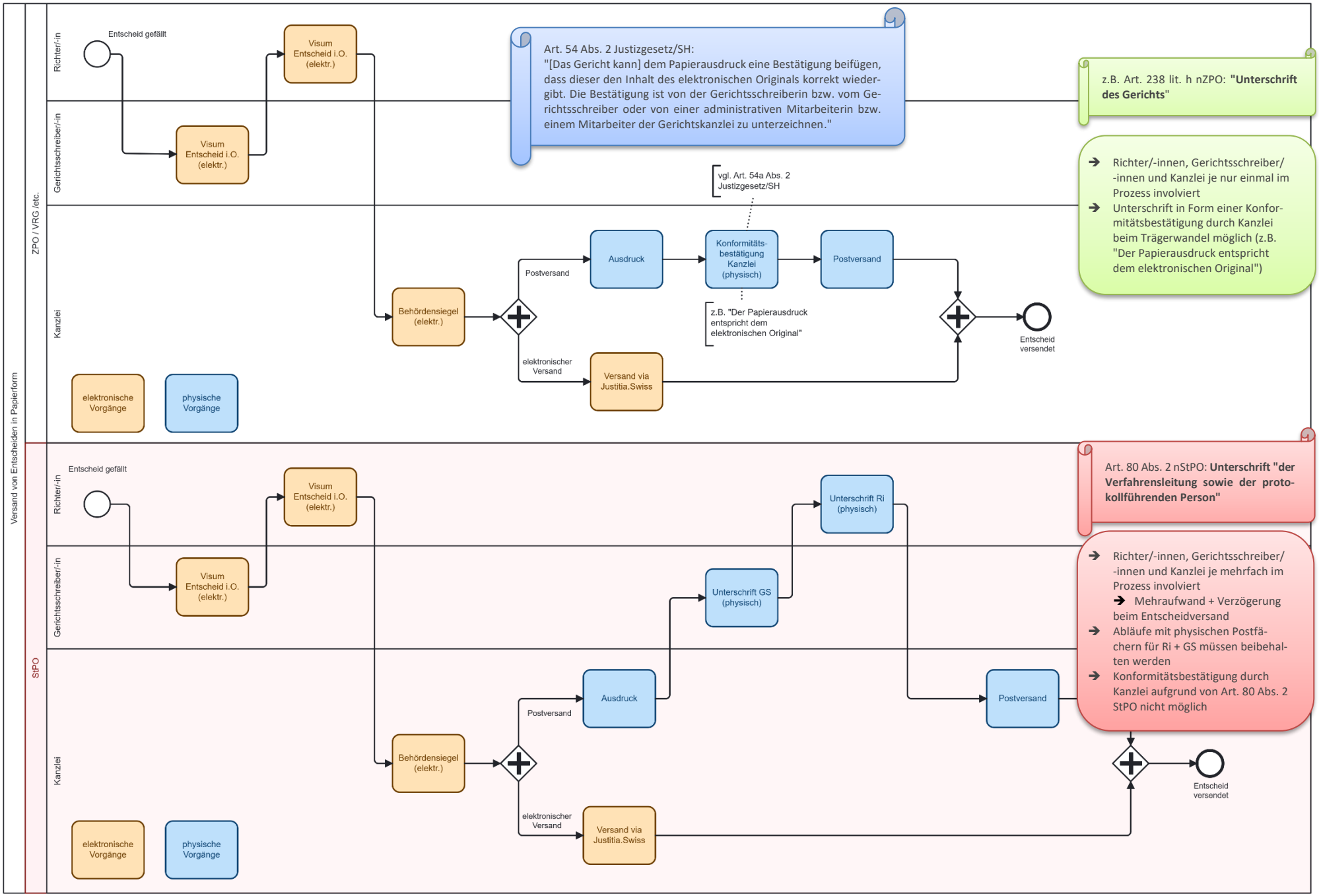
Freundliche Grüsse
OBERGERICHT DES KANTONS SCHAFFHAUSEN

Präsidentin	Leitender Gerichtsschreiber
Annette Dolge	Patrick Honegger-Müntener

OBERGERICHT * DES KANTONS SCHAFFHAUSEN *

Kopie an Amt für Justiz und Gemeinden (natascha.wermelinger@sh.ch)
Kantonsgericht (andreas.textor@sh.ch)
Kindes- und Erwachsenenschutzbehörde (denise.freitag@sh.ch)
Staatsanwaltschaft (peter.sticher@sh.ch)

Anhang (Versand in Papierform)



privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Eidgenössisches Justiz- und Polizeidepartement EJPD

Per Mail:
cornelia.perler@bj.admin.ch

Bern, 22. Juni 2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ): Vernehmlassung

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur erwähnten Vorlage Stellung nehmen zu können. Aus datenschutzrechtlicher Sicht ergeben sich die nachfolgenden Anträge und Hinweise.

Allgemeine Feststellungen:

Das Bundesgesetz vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ; SR 172.023) setzt den Rahmen für zwei Arten von digitalen Lösungen. Gemäss dem Zweckartikel (Art. 1 Abs. 2 Bst. a BEKJ) sollen eine oder mehrere Plattformen für die elektronische Übermittlung von Dokumenten in der Justiz aufgebaut und betrieben werden. Dabei soll gemäss Art. 3 BEKJ eine zentrale Plattform von einem Bundesorgan – auch für den kantonalen Vollzug – angeboten werden. Diese befindet sich mit Justitia.Swiss derzeit im Aufbau und kann sowohl von Bundesbehörden als auch von kantonalen Behörden im Sinne einer Aufgabenübertragung an die zu gründende öffentlich-rechtliche Körperschaft genutzt werden.

Zum anderen legitimiert Art. 5 BEKJ die öffentlich-rechtliche Körperschaft, dass sie neben der zentralen Plattform zusätzliche Dienstleistungen und technische Mittel anbieten kann, die für die elektronische Kommunikation in Justizverfahren spezifisch geeignet sind. Diese können von Bundesorganen sowie kantonalen öffentlichen Organen im Rahmen einer Auftragsdatenbearbeitung genutzt werden, wobei die öffentlichen Organe gemäss ihrem eigenen Datenschutzgesetz verantwortlich bleiben.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

Beide Arten von Diensten betreffen gemäss dem verabschiedeten Gesetz ausschliesslich Justiz- und Verwaltungsjustizverfahren. Alle anderen Verfahren sind vom BEKJ ausgenommen. Für Verwaltungsverfahren des Bundes sieht eine indirekte Änderung des VwVG eine eigene Plattform vor, die von einer vom Bundesrat beauftragten Verwaltungseinheit der zentralen Bundesverwaltung betrieben wird; dabei werden die Vorschriften des BEKJ – ohne jene zur Trägerschaft – als anwendbar erklärt (Art. 6a VwVG). Der vorliegende Vorentwurf der VEKJ dient hauptsächlich der Umsetzung des BEKJ, erweitertet aber auch den Geltungsbereich um (bundesrechtliche) Verwaltungsverfahren.

Gemäss aktuellem Wissenstand von privatim wird in Betracht gezogen, dass für Verwaltungsverfahren dieselbe Plattform wie für Justizverfahren genutzt werden soll. Auch wenn ein solcher Ansatz als sinnvoll erscheinen mag, wird dies nach Einschätzung von privatim nicht umsetzbar sein oder zumindest für gross Komplikationen sorgen. Dies würde bedeuten, dass dieselbe Plattform sowohl als Aufgabe der öffentlich-rechtlichen Körperschaft in eigener Verantwortung als auch im Rahmen einer Auftragsdatenbearbeitung unter Verantwortung des noch zu bestimmenden Bundesorgans genutzt werden müsste.

Sollten auch kantonale öffentliche Organe die Plattform nutzen können, stellen sich dieselben Fragen.

Privatim empfiehlt daher zu prüfen, inwieweit die öffentlich-rechtliche Körperschaft überhaupt Dienstleistungen anbieten kann, die über die gesetzlichen Vorgaben hinausgehen.

Unter Berücksichtigung der aktuellen Grundlagen empfiehlt privatim zudem eine klare organisatorische und technische Entflechtung und Trennung der Plattformen für die Kommunikation in Justiz- und in Verwaltungsverfahren. Auch sollte eine Anpassung des BEKJ geprüft werden, damit die Plattform auf einer ausreichenden gesetzlichen Grundlage, wie die zusätzlichen Dienstleistungen gemäss Art. 5, auch für andere Verfahren anbieten und von öffentlich-rechtlichen Körperschaften genutzt werden kann. Schliesslich sind die Abgrenzungen zwischen den aufsichtsrechtlichen Kompetenzen der kantonalen Datenschutzbehörden und des EDÖB nicht klar, weshalb eine Klarstellung im Rahmen einer Verordnung im Sinne von Art. 33 des Bundesgesetzes über den Datenschutz erfolgen sollte.

Verschlüsselung und Virenprüfung

Art. 14 verpflichtet die Anbieterin, beim Empfang von Dokumenten eine Virenprüfung durchzuführen. Gemäss dem aktuellen Informationsstand von privatim ist die Justitia-Plattform so konzipiert, dass jedes Dossier mit einem eigenen Schlüssel verschlüsselt wird. Damit scheinen die technischen Voraussetzungen für die Implementierung einer Ende-zu-Ende-Verschlüsselung grundsätzlich gegeben zu sein. Bei einer solchen Verschlüsselung würden die Daten bereits bei der absendenden Partei verschlüsselt und könnten ausschliesslich von der empfangenden Partei entschlüsselt werden. Die Pflicht zur Virenprüfung führt jedoch dazu, dass die Dokumente bei der Anbieterin als Klartext vorliegen müssen, und verhindert damit die Umsetzung einer echten Ende-zu-Ende-Verschlüsselung.

Aufgrund der Ausnahmen gemäss Art. 14 Abs. 2 und 3 muss zudem davon ausgegangen werden, dass die Virenprüfung nicht in jedem Fall durchgeführt werden kann. Weiter kann angenommen werden, dass sowohl die absendende als auch die empfangende Partei die Dokumente ihrerseits einer Virenprüfung unterziehen. Vor diesem Hintergrund erscheint fraglich, ob der Nutzen dieser zusätzlichen Virenprüfung den Verlust an Vertraulichkeitsschutz, der durch den Verzicht auf eine Ende-zu-Ende-Verschlüsselung entsteht, aufzuwiegen vermag.

privatim empfiehlt daher zu prüfen, ob eine Ende-zu-Ende-Verschlüsselung eingeführt werden kann. Dies könnte mit einer Verpflichtung der Nutzerinnen und Nutzer der Plattform verbunden werden, die Dokumente vor dem Versand beziehungsweise nach dem Empfang einer Virenprüfung zu unterziehen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

Alexis Roussel
Place Numa-Droz 2
2000 Neuchâtel

Neuchâtel, le 20 juin 2026

Office fédéral de la justice (OFJ)
À l'attention de Mme Cornelia Perler
cornelia.perler@bj.admin.ch

Objet : Contribution personnelle à la consultation publique sur l'avant-projet d'ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP), exécutant la loi fédérale du 20 décembre 2024 sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ, RS 172.023)

Madame, Monsieur,

J'ai l'honneur de vous adresser ma contribution personnelle à la consultation ouverte le 13 mars 2026 par le Département fédéral de justice et police. L'avant-projet OCEP fixe les conditions techniques, organisationnelles et procédurales de la communication électronique entre les parties (avocats, autorités, professionnels assujettis), les juridictions et les autorités administratives fédérales. C'est l'un des chantiers les plus structurants de la justice suisse. Il rend la communication électronique obligatoire pour les professionnels assujettis dans les procédures fédérales.

Ma démarche est citoyenne et professionnelle. Je dirige les opérations de Nym Technologies SA, infrastructure d'anonymisation des communications. Je siège au Conseil d'orientation stratégique de l'Institut des droits fondamentaux du numérique (iDFrights). J'ai présidé le Parti pirate suisse dont je suis membre. J'ai contribué aux travaux qui ont conduit à l'inscription du droit à l'intégrité numérique à l'art. 21A de la Constitution genevoise (votée le 18 juin 2023, près de 94 % de oui) et à l'art. 10a de la Constitution neuchâteloise (votée le 24 novembre 2024, 91,5 % de oui). Je suis co-auteur, avec Grégoire Barbey, de *Notre si précieuse intégrité numérique* (Slatkine, 2021). Je détiens un master 2 en droit public des nouvelles technologies. J'ai travaillé pour les Nations Unies au Sommet mondial de la société de l'information (Genève 2003 et Tunis 2005).

Cette contribution s'articule en huit points. 1. La numérisation de la justice doit incarner le droit à l'intégrité numérique. 2. Garantir la voie papier équivalente pour les justiciables non professionnels. 3. Le chiffrement de bout en bout est une condition d'indépendance. 4. Souveraineté numérique de la justice. 5. Lacunes du dossier de consultation. 6. Articulation avec les Constitutions cantonales. 7. Propositions de modification de l'OCEP. 8. Recommandations institutionnelles.

1. La numérisation de la justice doit incarner le droit à l'intégrité numérique

Le droit à l'intégrité numérique de la personne se rattache au droit à la vie (art. 10 Cst.) et au droit à la sphère privée (art. 13 Cst.). Il est consacré à l'art. 21A Cst-GE et à l'art. 10a Cst-NE. Il prolonge la Convention 108+ du Conseil de l'Europe. Il comporte cinq composantes opératoires :

protection contre le traitement abusif des données, sécurité dans l'espace numérique, droit à une vie hors ligne, droit à l'oubli, droit à ne pas être mesuré, analysé ou surveillé.

La justice est un domaine où ces composantes se rencontrent toutes. Les dossiers contiennent des données ultra-sensibles (procédures pénales, civiles, faillites, victimes au sens de la LAVI). Les avocats relèvent du secret professionnel (art. 13 LLCA). L'accès au juge est un droit fondamental (art. 29a Cst., art. 6 CEDH). La numérisation peut renforcer ces garanties ou les abîmer. La rédaction de l'OCEP fait la différence.

L'avant-projet n'évoque ni les Cst-GE et Cst-NE, ni le droit à l'intégrité numérique, ni la jurisprudence européenne pertinente, notamment l'arrêt Big Brother Watch et al. c. Royaume-Uni (CEDH, GC, 25 mai 2021) sur la surveillance de masse et le secret professionnel des avocats, ainsi que les arrêts Klass et autres c. Allemagne (CEDH, 6 septembre 1978) et Roman Zakharov c. Russie (CEDH, GC, 4 décembre 2015) sur les garanties contre la surveillance. Cette omission n'est pas une simple lacune rédactionnelle. Elle révèle une conception de la numérisation comme efficacité administrative. Elle doit être corrigée.

2. Garantir la voie papier équivalente pour les justiciables non professionnels

L'art. 37 LPCJ rend la communication électronique obligatoire pour les professionnels assujettis (avocats, autorités, fiduciaires) à l'expiration des délais transitoires. Les justiciables non professionnels ne sont pas concernés par cette obligation. C'est le cas pour la majorité des justiciables, notamment des particuliers en procédure civile, en procédure pénale comme partie civile, en procédure d'exécution forcée comme débiteur, en procédure d'aide aux victimes au sens de la LAVI.

L'avant-projet doit garantir que la voie papier reste pleinement ouverte et équivalente en termes de droits procéduraux pour ces justiciables. Cette garantie n'est nulle part dans le texte. La pratique cantonale en matière de cyberadministration montre que la fracture numérique frappe les personnes âgées, les personnes en situation de précarité, les personnes en situation de handicap, et les personnes peu familières du numérique. Des précédents à Neuchâtel illustrent exactement ce qu'il ne faut pas faire : exercer son droit ne doit pas coûter de l'argent ni du temps supplémentaires avec, par exemple, des émoluments moins chers pour un guichet numérique.

Sous l'angle de l'art. 29a Cst. (garantie de l'accès au juge), du droit à une vie hors ligne (art. 21A Cst-GE et art. 10a Cst-NE) et du principe d'égalité (art. 8 Cst.), le maintien d'une voie papier gratuite et équivalente est une condition matérielle de la légitimité de l'OCEP.

3. Le chiffrement de bout en bout est une condition d'indépendance

L'art. 2 al. 1 du projet impose la protection contre les accès et modifications non autorisés (let. a) et le chiffrement selon les normes techniques de l'administration fédérale (let. b). La rédaction est insuffisante au regard de la sensibilité des contenus traités.

La distinction entre chiffrement en transit et chiffrement de bout en bout est essentielle. Le chiffrement en transit protège la communication entre l'utilisateur et la plateforme. Le chiffrement de bout en bout protège le contenu contre l'exploitant lui-même et ses sous-traitants. Le chiffrement de bout en bout dont il est question ici n'exclut évidemment pas les destinataires légitimes du document (avocat, tribunal, autres parties à la procédure), qui doivent accéder au contenu pour exercer leurs droits ou leurs missions. Il vise à exclure les acteurs intermédiaires (exploitant, sous-traitants, autorité étrangère exerçant un pouvoir extraterritorial sur l'opérateur).

C'est une condition de l'indépendance des tribunaux (art. 191c Cst.) et du secret professionnel des avocats.

Les clés de chiffrement doivent rester sous le contrôle des parties à la procédure (avocats, autorités, autres parties), à l'exclusion de la plateforme et de ses sous-traitants. À défaut, l'OCEP doit exiger un audit indépendant attestant que l'exploitant ne dispose pas d'accès en clair au contenu, et que les sauvegardes et caches respectent ce principe.

4. Souveraineté numérique de la justice

La plateforme centralisée Justitia.Swiss et les autres plateformes autorisées doivent être hébergées et opérées exclusivement sur sol suisse. L'opérateur doit être une entité de droit suisse, dont l'infrastructure est exploitée en Suisse et soumise exclusivement à la juridiction suisse, à l'exclusion de toute loi extraterritoriale, notamment le CLOUD Act américain et les sections 702 et 703 du FISA Amendments Act, conformément à l'art. 271 CP.

Cette exigence n'est pas une question technique secondaire. Elle a une portée constitutionnelle. L'art. 191c Cst. consacre l'indépendance des tribunaux. Une plateforme judiciaire soumise à des injonctions extraterritoriales ne respecte pas cette indépendance. La jurisprudence européenne le confirme : dans Schrems II (CJUE, GC, 16 juillet 2020, C-311/18), la Cour a constaté l'incompatibilité entre les programmes de surveillance américains (FISA section 702, Executive Order 12333) et les garanties européennes en matière de protection des données. Cette incompatibilité s'applique a fortiori aux plateformes judiciaires. Le précédent de l'appel d'offres fédéral attribué à IBM, AWS, Oracle, Azure et Alibaba doit servir d'avertissement, pas de modèle. La fuite Xplain (2023), qui a touché des données de fedpol et de l'OFJ, démontre par ailleurs que les chaînes de sous-traitance créent des points de compromission.

La LMETA (RS 172.019) art. 9 al. 1 pose le principe de la publication en source ouverte du code des logiciels développés par ou pour la Confédération, sous réserve de droits de tiers et d'impératifs de sécurité. L'OCEP doit appliquer ce principe aux composants critiques de Justitia.Swiss et des autres plateformes autorisées.

5. Lacunes du dossier de consultation

Le dossier présente plusieurs lacunes auxquelles l'OFJ doit répondre :

a) **Aucune analyse d'impact relative à la protection des données** au sens de l'art. 22 nLPD pour la plateforme Justitia.Swiss, alors que la centralisation de la communication judiciaire fédérale remplit tous les critères matériels du traitement à risque élevé.

b) **Aucune référence aux Cst-GE et Cst-NE** qui consacrent le droit à l'intégrité numérique et auxquelles sont liés les avocats inscrits aux barreaux cantonaux genevois et neuchâtelois.

c) **Aucune obligation explicite de chiffrement de bout en bout**, alors que la sensibilité des dossiers judiciaires l'exige et que la formule « chiffrement selon les normes techniques de l'administration fédérale » est trop souple.

d) **Aucune obligation de localisation et d'opération sur sol suisse** sous la seule juridiction suisse, à l'abri du CLOUD Act et des autres lois extraterritoriales.

e) **Aucune obligation de standards ouverts ni de publication du code source** en application de l'art. 9 al. 1 LMETA, alors que les composants critiques d'une plateforme judiciaire doivent pouvoir être audités indépendamment.

f) **Aucune garantie écrite de la voie papier équivalente** pour les justiciables non professionnels.

g) **Délégation excessive au DFJP** (art. 2 al. 2 du projet) sur des paramètres techniques essentiels qui touchent aux droits fondamentaux et qui devraient relever de la loi formelle au sens de l'art. 164 al. 1 let. b et c Cst.

h) **Pas de bilan des incidents récents** qui devraient pourtant éclairer la conception : Xplain (2023, données fedpol et OFJ) et France-Travail (mars 2024, environ 43 millions de personnes).

i) **Aucune articulation explicite avec ZertES (RS 943.03)** sur la signature électronique qualifiée, ni avec l'art. 130 CPC et l'art. 86 CPP qui régissent déjà la transmission électronique d'écrits dans les procédures civiles et pénales. L'OCEP doit s'inscrire dans ce paysage normatif et non créer un régime parallèle qui pourrait fragiliser les automatismes existants.

6. Articulation avec les Constitutions cantonales

Les avocats inscrits aux barreaux cantonaux genevois et neuchâtelois exercent dans des cantons garantissant constitutionnellement le droit à l'intégrité numérique. Les justiciables résidant dans ces cantons bénéficient de la même garantie. La Confédération doit en tenir compte quand elle conçoit une plateforme nationale qui s'imposera aux acteurs cantonaux concernés.

Dans un esprit de coopération fédérale et de bonne foi au sens de l'art. 44 al. 2 Cst., et sans porter atteinte à la primauté du droit fédéral en matière procédurale (art. 49 al. 1 Cst.), la Confédération doit, dans l'exercice de sa propre compétence, tenir compte des engagements constitutionnels cantonaux relatifs à l'intégrité numérique. L'OCEP doit notamment prévoir, par voie d'interprétation conforme et par convention de coordination, le maintien d'un canal non numérique gratuit pour les justiciables domiciliés dans les cantons concernés. Le PFPDT et les Préposés cantonaux concluent à cet effet une convention.

7. Propositions de modification de l'OCEP

7.1. Voie papier équivalente pour les justiciables non professionnels (nouvel art.)

> *Art. X (nouveau) : 1. Les justiciables qui ne sont pas tenus d'utiliser une plateforme conservent en tout temps le droit de communiquer avec les juridictions et les autorités par voie postale, sans surcoût ni délai supplémentaire. 2. Aucune sanction, irrecevabilité ou conséquence procédurale défavorable ne peut résulter de l'usage de la voie postale par un justiciable non professionnel. 3. Les juridictions et autorités maintiennent un guichet physique accessible, permettant le dépôt, la consultation et l'impression des pièces, sans frais.*

7.2. Conditions techniques renforcées (modification de l'art. 2 al. 1)

> *Art. 2 al. 1 (modifié) : Les plateformes doivent remplir les exigences suivantes en plus de celles prévues dans la LPCJ :*
>
> *a. les documents sont protégés contre tout accès et toute modification non autorisés par des tiers, y compris l'exploitant de la plateforme et ses sous-traitants.*
>
> *b. les documents sont chiffrés de bout en bout selon les normes techniques de l'administration fédérale. Les clés de chiffrement sont sous le contrôle des parties à la procédure. Les documents sont transmis sous forme chiffrée.*

c. la plateforme peut réceptionner et transmettre des documents d'une taille maximale de 2 gigaoctets.

d. les utilisateurs peuvent supprimer en tout temps les documents et quittances qui figurent dans le compte utilisateur. Cette suppression entraîne la destruction effective dans tous les systèmes de la plateforme, y compris caches, sauvegardes et journaux applicatifs au-delà d'un délai de 90 jours.

e. les documents et métadonnées peuvent être exportés par l'utilisateur dans un format standard ouvert (PDF/A, JSON, XML) à des fins de portabilité.

7.3. Hébergement et opération sur sol suisse (nouvel art. 2a)

Art. 2a (nouveau) : 1. La plateforme centralisée et les autres plateformes autorisées sont hébergées et opérées exclusivement sur sol suisse, par une entité de droit suisse dont l'infrastructure est exploitée en Suisse et soumise exclusivement à la juridiction suisse, à l'exclusion de toute loi extraterritoriale, conformément à l'art. 271 CP. 2. Toute requête d'autorité étrangère portant sur des données stockées sur la plateforme est traitée exclusivement par la voie de l'entraide judiciaire internationale. 3. L'opérateur certifie annuellement, sous peine de retrait de l'autorisation, l'absence de transmission de données à des autorités étrangères en dehors de la voie de l'entraide.

7.4. Standards ouverts, code source, audit (nouvel art. 2b)

Art. 2b (nouveau) : 1. La plateforme repose sur des standards ouverts et publiés. Les composants critiques (chiffrement, signatures, identification, journaux) sont fondés sur des logiciels libres ou, à défaut, sur du code dont les sources sont disponibles à l'audit indépendant, conformément à l'art. 9 al. 1 LMETA (RS 172.019), sous réserve de droits de tiers et d'impératifs de sécurité. 2. Un audit de sécurité et de conformité est réalisé tous les deux ans par un organisme certifié indépendant. Le rapport est public dans la mesure compatible avec la sécurité opérationnelle. 3. La plateforme respecte au minimum les normes eCH-0059 et WCAG 2.2 d'accessibilité. Un audit annuel d'accessibilité est publié.

7.5. Identification minimisée (nouvel art. 2c)

Art. 2c (nouveau) : 1. L'identification sur les plateformes peut se faire par e-ID, par identifiant alternatif équivalent (numéro inscrit au registre cantonal des avocats au sens de l'art. 4 LLCA, numéro UID pour les autorités et personnes morales) ou par un autre moyen reconnu par le DFJP. L'usage du numéro AVS comme identifiant universel reste limité aux finalités prévues par la loi fédérale du 18 juin 2010 sur le numéro AVS (LNAVS, RS 431.112.1). 2. Les attributs d'identification transmis sont limités à ceux strictement nécessaires à la qualité dans la procédure (identité, qualité d'avocat, qualité d'autorité). L'enrichissement par recoupement avec d'autres bases publiques est interdit. 3. Les identifiants utilisés sur une plateforme sont pseudonymisés et spécifiques à cette plateforme. Aucun identifiant unique n'est réutilisé entre plateformes différentes.

7.6. Surveillance par le PFPDT (nouvel art. 2d)

Art. 2d (nouveau) : 1. Le PFPDT, déjà compétent au titre des art. 43 ss nLPD, exerce une surveillance permanente sur les plateformes autorisées. Il est consulté préalablement à toute autorisation et à toute évolution majeure des plateformes. 2. Le DFJP communique annuellement au PFPDT les données statistiques sur l'usage des plateformes, les incidents de sécurité et les recours déposés. 3. Le DFJP publie chaque

année un rapport public sur l'usage des plateformes, dans la mesure compatible avec la confidentialité des procédures.

7.7. Articulation avec les Constitutions cantonales (nouvel art. 2e)

Art. 2e (nouveau) : Dans un esprit de coopération fédérale et de bonne foi au sens de l'art. 44 al. 2 Cst., et sans porter atteinte à la primauté du droit fédéral (art. 49 al. 1 Cst.), la Confédération tient compte, dans l'application de la présente ordonnance, des engagements constitutionnels cantonaux relatifs à l'intégrité numérique. Pour les parties domiciliées dans un canton concerné, le maintien d'un canal non numérique gratuit est garanti par voie d'interprétation conforme et par convention. Le PFPDT et les Préposés cantonaux concluent à cet effet une convention.

7.8. Privacy by design et by default (nouvel art. 2f)

Art. 2f (nouveau) : Les plateformes mettent en œuvre le principe de protection des données dès la conception et par défaut au sens de l'art. 7 nLPD pour toute fonctionnalité nouvelle. Les paramètres par défaut sont les plus protecteurs (minimisation, conservation limitée, accès restreint).

8. Recommandations institutionnelles

Au-delà des modifications de texte ci-dessus, je vous demande de :

a) **réaliser une analyse d'impact LPD complète** au sens de l'art. 22 nLPD pour la plateforme Justitia.Swiss, conjointement avec le PFPDT, et la rendre publique avant l'adoption de l'OCEP.

b) **auditer indépendamment Justitia.Swiss** dans son architecture pré-déploiement, avec rapport public dans la mesure compatible avec la sécurité.

c) **auditionner les ordres d'avocats cantonaux** et les associations de défense des justiciables sur le caractère effectif de la voie papier et l'accessibilité de la plateforme.

d) **auditionner le PFPDT et les Préposés cantonaux** sur les modalités de surveillance et la rédaction de la convention de coordination.

e) **intégrer le bilan des incidents récents** (Xplain 2023 et autres failles majeures en Suisse et en Europe) dans la conception architecturale de la plateforme.

f) **inscrire dans le rapport explicatif final** l'articulation avec les art. 21A Cst-GE et 10a Cst-NE et avec la jurisprudence européenne pertinente.

9. Conclusion

La numérisation de la justice peut renforcer l'accès au juge ou y faire obstacle. Elle peut consolider l'indépendance des tribunaux ou la fragiliser par dépendance à des opérateurs étrangers. Elle peut servir les justiciables ou les exclure. La rédaction de l'OCEP fait la différence.

Je vous demande d'inscrire dans l'OCEP les huit propositions ci-dessus : voie papier équivalente, chiffrement de bout en bout, hébergement souverain hors CLOUD Act, standards ouverts au sens de l'art. 9 LMETA, identification minimisée, surveillance PFPDT, articulation avec les Cst-GE et Cst-NE, privacy by design. Je vous demande aussi de mettre en œuvre les six recommandations institutionnelles. Ces ajouts ne s'opposent pas à la modernisation de la justice. Ils en sont la condition.

Je me tiens à votre disposition pour tout échange complémentaire.

Je vous prie d'agréer, Madame, Monsieur, l'expression de ma considération distinguée.

Alexis Roussel
Directeur des opérations, Nym Technologies SA
Membre du Conseil d'orientation stratégique de l'iDFrights

SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Département fédéral de Justice et Police DFJP

Transmis par courriel:
cornelia.perler@bj.admin.ch

GR/RR

Berne, le 18 juin 2026

Prise de position de la Fédération suisse des avocats (FSA) relative à l'Ordonnance sur la communication électronique dans les procédures judiciaires et administratives régies par le droit fédéral (OCEP)

Monsieur le Conseiller fédéral,
Mesdames, Messieurs,

La Fédération suisse des avocats (FSA) vous remercie de lui avoir donné l'occasion de prendre position dans le cadre de la consultation susmentionnée.

1. Remarques générales

Les observations qui suivent visent à améliorer la sécurité juridique, la cohérence entre le texte de l'ordonnance et le rapport explicatif, ainsi que l'adéquation des règles aux besoins de la pratique. Elles sont présentées article par article.

À titre liminaire, pour plus de clarté de l'ordonnance, il apparaît opportun que celle-ci indique, pour chaque article de celle-ci, à quel article de la loi elle fait référence. Ceci à l'instar, par exemple, de l'OSFin indiquant, après chaque article, à quel article la LSFin l'article de l'OSFin se rapporte.

2. Remarques par article

2.1 Art. 2 – Conditions techniques et fonctionnalités de la plateforme

Al. 2, let. c (taille des fichiers) – La FSA estime que la limite maximale de 2 Go par fichier n'est pas adaptée aux besoins de la pratique. Dans de nombreuses procédures – notamment lorsque des preuves sous forme de vidéos, d'images en haute résolution ou de dossiers volumineux doivent être produites – cette limite s'avère insuffisante et ne correspond plus aux standards techniques actuels. Une restriction trop basse de la taille des fichiers constitue par ailleurs un obstacle concret à l'utilisation de la communication électronique par les praticiens ; l'expérience passée a montré que de telles limitations peuvent freiner significativement l'adoption de ces outils.

En outre, le rapport explicatif mentionne l'existence de possibilités permettant la transmission de fichiers de plus grande taille, alors que le texte de l'ordonnance ne prévoit pas de telles modalités. Cette incohérence nuit à la sécurité juridique. Les conditions et modalités de transmission des fichiers dépassant la limite fixée devraient dès lors être expressément réglées dans l'ordonnance elle-même ou, à tout le moins, dans l'ordonnance du DFJP. En conséquence, soit la taille maximale des fichiers devrait être sensiblement augmentée, soit une solution alternative fiable et clairement réglementée devrait être prévue afin de permettre la transmission de fichiers dépassant cette limite, et ce pour l'ensemble des parties à la procédure.

Al. 2 (exigences déléguées au DFJP) – Il doit également être possible de se prononcer, dans le cadre d'une procédure de consultation, sur les exigences relatives à la plateforme qui doivent encore être définies par le DFJP. Le fait de déplacer au niveau du département la réglementation des exigences relatives aux interfaces et aux fonctionnalités opérationnelles est délicat s'il a pour conséquence de soustraire cette réglementation à la procédure de consultation.

2.2 Art. 3 – Autorisation et conditions

Al. 4 – Suggestion d'ajout, pour plus de clarté : « Il retire l'autorisation s'il constate que les conditions posées à l'art. 25 LPCJ et à l'art. 2 de la présente ordonnance ne sont plus remplies ».

2.3 Art. 4 – Documents, annexes et formats

Al. 1 et 2 (documents / annexes) – La distinction entre « documents » (al. 1) et « annexes » (al. 2) n'est pas claire et a une incidence concrète, dès lors que les « documents » sont soumis à une forte restriction de format.

Al. 2 (champ d'application) – Il n'est pas clair si cet alinéa est également applicable aux autorités.

Al. 3 (formats admis) – Les formats courants de traitement de texte (.doc, .docx [Microsoft Word], .odt [LibreOffice Writer et OpenOffice], .pages [Apple Pages], .rtf, .txt), de feuilles de calcul (.xls, .xlsx [Microsoft Excel], .ods [LibreOffice Calc et OpenOffice], numbers [Apple Numbers], .csv) et de diaporamas (.ppt, .pptx [Microsoft PowerPoint], .odp [LibreOffice

Impress et OpenOffice], .key [Apple Keynote]) devraient être admis. La liste des formats courants devrait donc être complétée en conséquence.

Al. 4 (format imposé pour les annexes) – Le texte prévoit que « l'autorité demande à la personne ou à l'autorité qui a remis l'annexe de la renvoyer dans un format déterminé ou d'y donner accès de façon adaptée ». Seule la dernière option est acceptable : on ne peut pas demander aux parties de modifier leurs offres de preuve.

Proposition de formulation pour l'al. 4 : « Lorsqu'une annexe est remise dans un autre format et que l'autorité chargée de la conduite de la procédure ne peut pas la lire, elle invite la personne ou l'autorité qui l'a remise à donner accès à l'annexe d'une manière appropriée. »

2.4 Art. 5 – Quittance

Al. 2, let. b et let. g (mention de la personne en cas d'accès par API) – Il ne paraît pas opportun de faire figurer sur la quittance le nom de la personne au nom de laquelle un document est envoyé ou consulté lorsque l'accès à la plateforme se fait par API. Dans ce cas, le nom de la personne physique ayant délégué ses droits au profil technique utilisé pour l'accès à l'API (cf. art. 10 OCEP) apparaîtrait sur toutes les quittances. Tel sera notamment le cas pour les grandes études d'avocats, qui communiqueront vraisemblablement avec la plateforme exclusivement par l'API. Le cas échéant, seul le nom de l'organisation pourrait figurer sur les quittances.

Al. 2, let. d, ch. 3 (rejet par l'antivirus) – Cette disposition présente un risque au regard du respect du délai. Il est dès lors nécessaire de préciser la date et l'heure exactes du rejet des documents par l'antivirus.

Al. 2, let. g (notion de « personne ») – Le cas visé par l'art. 5, al. 2, let. G n'est pas très compréhensible, ni la référence à la « personne » ; par opposition, l'al. 2, let. b paraît plus clair, et le rapport explicatif (p. 17) n'aide pas à comprendre cette notion. Il apparaît que les cas visés sont les cas de délégation : il conviendrait dès lors de clarifier la formulation en ce sens, afin de lever toute ambiguïté.

Al. 3 (quittances contradictoires) – Il serait précautionneux de prévoir une primauté de la quittance lisible par l'humain en cas de contradiction (même si une telle hypothèse est improbable).

2.5 Art. 6 – Forme du cachet

La forme du cachet ne semble pas traitée. Il avait été évoqué que le cachet devrait être visible par l'humain et compréhensible comme tel. Comme cela ressort des dispositions finales relatives aux dispositions modifiées, ce point est peut-être réglé par l'OFCOM en vertu de l'art. 14b de l'ordonnance sur la signature électronique ; on pourrait toutefois prévoir ici des exigences à l'adresse de l'OFCOM sur la forme du cachet.

Par ailleurs, une divergence apparaît entre le texte de l'ordonnance et le rapport explicatif s'agissant de l'apposition du cachet et de l'horodatage. Alors que le texte de l'ordonnance semble admettre qu'un seul document soit muni d'un cachet et d'un horodatage, le rapport explicatif laisse entendre que l'autorité devrait apposer ces éléments sur l'ensemble des documents. Cette incohérence appelle une clarification afin d'assurer la sécurité juridique et une application uniforme.

2.6 Art. 7 – Modalités d'apposition du cachet électronique

La FSA relève une incertitude quant aux modalités d'apposition du cachet électronique au regard des explications figurant dans le rapport explicatif (p. 18). En particulier, il n'est pas clairement établi si le cachet doit être apposé systématiquement sur un document séparé ou uniquement lorsque plusieurs documents sont transmis. Une interprétation a contrario pourrait conduire à considérer que, dans le cas de la transmission d'un seul document, celui-ci serait directement muni d'un cachet et d'un horodatage. Une telle approche soulève toutefois des réserves, dans la mesure où elle serait susceptible de contrevenir au principe selon lequel les documents ne devraient pas être modifiés par la plateforme.

2.7 Art. 8 – Indisponibilité de la plateforme et sécurité

Al. 1 (panne d'AGOV) – Une panne d'AGOV devrait être assimilée à une panne de la plateforme. Il s'agit d'éviter l'argument selon lequel une panne d'AGOV ne constituerait pas une panne de la plateforme et ne justifierait donc pas une restitution de délai, alors que, de facto, une panne d'AGOV équivaut à une impossibilité d'accéder à la plateforme. Il pourrait être opportun d'intégrer l'établissement de protocoles de disponibilité et d'incidents. Cela permettrait, à tout le moins dans le cadre d'une procédure de restitution de délai, d'apporter des éléments de preuve quant à l'indisponibilité du système.

Al. 3 (niveau de protection) – Il conviendrait d'ajouter « un niveau de protection adapté et adéquat ». Par ailleurs, le terme « adapté » semble imprécis : adapté à quoi ? Adapté aux risques.

2.8 Art. 9 – Compte utilisateur et désignation du cachet

Al. 1 – La formulation est imprécise et devrait préciser : « dans le compte utilisateur lié à leur identité électronique ».

Al. 2, let. c (désignation du cachet) – La portée de la notion de « désignation du cachet » n'est pas claire. S'agit-il de la clé publique (public key) permettant de vérifier le cachet de l'autorité ? Une clarification serait bienvenue.

Al. 3, let. b (profil pour les organisations) – Il n'est pas encore définitivement établi s'il existera un profil pour les organisations. Pour les avocats, ce sera l'avocat lui-même. Ce point devra être clarifié plus précisément dans le cadre du projet.

2.9 Art. 11 – Confirmation et inactivité

Le délai de trois mois jusqu'au retrait automatique des autorisations apparaît bref au regard de la sécurité juridique et de l'utilisation pratique de la plateforme, en particulier lorsque l'invitation à confirmer les autorisations n'est adressée qu'une seule fois. La formulation « au moins une fois par an » n'exclut pas que cette invitation ne soit envoyée qu'une seule fois. Les avocates et avocats qui ne mènent que rarement des procédures et utilisent dès lors peu la plateforme pourraient facilement omettre une telle invitation, laquelle devrait vraisemblablement leur parvenir par courriel. Il en résulterait que des autorisations existantes pourraient être retirées uniquement en raison d'une confirmation omise. Il conviendrait dès lors de prévoir dans l'ordonnance l'octroi d'un bref délai supplémentaire, accompagné de l'indication qu'à défaut de confirmation dans ce délai, l'autorisation sera retirée. Une telle

solution permettrait de réduire le risque de blocages involontaires, sans porter atteinte à l'objectif poursuivi par le contrôle périodique des autorisations.

Al. 2 – La formulation est imprécise et devrait préciser : « trois mois après la dernière demande de confirmation restée vaine ».

2.10 Art. 14 – Documents rejetés par l'antivirus et respect du délai

Al. 5 – Cette disposition est à lire en parallèle avec l'art. 5, al. 2, let. d de l'ordonnance. Il apparaît important de préciser que le document est néanmoins réputé transmis.

C'est ce qui a été communiqué par divers canaux lors de la présentation de la problématique de l'antivirus. Cela correspond également au principe ancré dans la jurisprudence selon lequel l'avocat est réputé de bonne foi (TF, 4P.15/2006 du 18 avril 2006, c. 2.2 ; CHAPPUIS B./GURTNER J., La profession d'avocat, N 28). Il est d'ailleurs difficilement imaginable qu'un avocat corrompe sciemment un fichier au moyen d'un virus dans le seul but de sauvegarder un délai ; une telle manière de procéder ouvrirait du reste la porte à des sanctions disciplinaires (art. 12 let. a LLCA), voire pénales (art. 144bis CP).

À notre sens, l'ordonnance devrait prévoir qu'en cas de refus d'un document en raison de la détection d'un virus, la plateforme liste ces documents sur la quittance de l'art. 5 (ou sur une quittance séparée), avec indication de la valeur de hachage des fichiers en question. Indépendamment de la question de la présomption de transmission du fichier (« réputé transmis »), cette donnée – le hachage – coupera court à toute discussion si l'autorité ou une partie a des motifs sérieux de considérer que le document transmis séparément (par exemple par envoi physique) correspond au document rejeté par l'antivirus de la plateforme.

2.11 Art. 22 – Numérisation des documents

Al. 3 – Suggestion de précision : « Ils doivent être rendus indexables par la reconnaissance optique de caractères et présenter une profondeur de couleur d'au moins 8 bits et une résolution d'au moins 300 DPI ».

En vous remerciant de l'attention que vous porterez aux présentes remarques, nous vous prions de croire, Monsieur le Conseiller fédéral, Mesdames, Messieurs, à l'assurance de notre plus haute considération,

Président FSA
Georg Rauber



Secrétaire général FSA
René Rall



Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Bundesamt für Justiz
Frau Cornelia Perler
Bundesrain 2

3003 Bern
cornelia.perler@bj.admin.ch

Bern, 19. Juni 2026 sgv-Kl

Vernehmlassungsantwort: Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ).

Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 hat Eidgenössisches Justiz- und Polizeidepartement EJPD die interessierten Kreise eingeladen, sich zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) zu äussern.

Der Schweizerische Gewerbeverband sgv unterstützt die Verordnung, die der Umsetzung des Bundesgesetzes dient.

Mit dem Bundesgesetz über die Plattformen für die elektronische Kommunikation (BEKJ) hat das Parlament die Grundlagen geschaffen, um durchgängig digitale, medienbruchfreie Justizverfahren zu ermöglichen. Die Aktenführung erfolgt elektronisch. Damit wird ein Obligatorium zur elektronischen Kommunikation für die professionellen Rechtsanwenderinnen und -anwender eingeführt.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Urs Furrer
Direktor

Dieter Kläy
stv. Direktor, Ressortleiter

Als grösste Dachorganisation der Schweizer Wirtschaft vertritt der Schweizerische Gewerbeverband sgv über 230 Verbände und über 600 000 KMU, was einem Anteil von 99.8 Prozent aller Unternehmen in unserem Land entspricht. Im Interesse der Schweizer KMU setzt sich der sgv für optimale wirtschaftliche und politische Rahmenbedingungen sowie für ein unternehmensfreundliches Umfeld ein.

Die Schweizerische Post AG
Stab CEO
International and
Public Affairs
Wankdorfallee 4
3030 Bern

Telefon +41 79 503 16 09
www.post.ch

Die Schweizerische Post AG, Stab CEO PIA, Wankdorfallee 4, 3030 Bern

Eidg. Justiz- und Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundesrain 20
3003 Bern

Als PDF/Word an: cornelia.perler@bj.admin.ch

Datum 22. Juni 2026
Kontaktperson Patrizia Rentsch
E-Mail patrizia.rentsch@post.ch
Direktwahl 079 503 16 09

Stellungnahme der Schweizerischen Post zur Vernehmlassung über die Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, im Rahmen der Vernehmlassung über die Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung nehmen zu können.

Im heutigen Rechtsverkehr zwischen Privaten und Behörden sowie unter Behörden – ganz gleich ob physisch oder digital – spielt die Schweizerische Post eine zentrale Rolle als vertrauenswürdiger Kommunikationskanal. Gerichtsurkunden stellt die Post seit jeher in der ganzen Schweiz zuverlässig und pünktlich zu. Die Versandarten «Gerichtsurkunden» und «A-Post Plus» bieten Gerichtsorganen Gewähr für eine rechtsverbindliche Zustellung von Gerichtsdokumenten. Für Eingaben an Gerichte und Behörden ist die Versandart «Einschreiben» das Mittel der Wahl. Seit 2010 sodann betreibt die Post IncaMail als vom Bund anerkannte Zustellplattform für die sichere elektronische Zustellung im Rahmen von rechtlichen Verfahren. Die definitive Anerkennung von IncaMail im Jahr 2016 unterstreicht die digitale Kompetenz der Schweizerischen Post und ihre Ambition, sowohl bei Behörden wie auch in der Privatwirtschaft elektronische Post-Lösungen zu etablieren. Die Post hat für die Konformität und Anerkennung von IncaMail viel investiert.

Die Einführung der zentralen elektronischen Plattform justitia.swiss sowie eventuell weiteren Plattformen nach dem BEKJ und die damit verbundene Verordnung ist für die Post und ihre Tochtergesellschaft Tresorit mit massgebenden Konsequenzen verbunden. Unser Dienst IncaMail wird im Rahmen des elektronischen Rechtsverkehrs in juristischen Prozessen aufgrund des Wegfalls der relevanten rechtlichen Grundlagen nicht mehr verwendet werden können. Zu den Ausführungen betreffend Übergangsbestimmungen sowie zum skizzierten Vorgehen mit einem Organisationskonto und Konkretisierung der Schnittstellen auf der Plattform orten wir noch Klärungsbedarf bzw. führen wir einen Alternativvorschlag ins Feld.

1. Übergangsbestimmungen

Mit dem vollständigen Inkrafttreten des BEKJ und des VEKJ, voraussichtlich per 1. Juli 2027, entfallen die bisherigen gesetzlichen Grundlagen für die elektronische Kommunikation im Justizbereich – namentlich die VeÜ-VwV sowie die VeÜ-ZSSV. Damit verlieren die bisher zugelassenen Anbieter wie IncaMail oder PrivaSphere ihre rechtliche Grundlage für die zertifizierte Zustellung in Gerichts- und Verwaltungsverfahren. Da das BEKJ (Art. 37) für den obligatorischen Anschluss an die neue Plattform justitia.swiss eine Übergangsfrist von bis zu fünf Jahren vorsieht, ergibt sich zwangsläufig eine Phase, in der ein erheblicher Teil der Kantone und Gerichte noch nicht auf die neue Plattform migriert sein wird. In dieser Zwischenphase besteht kein klarer Rechtsrahmen für die elektronische Übermittlung von Rechtsschriften und anderen verfahrensrelevanten Dokumenten. Ein solches Regelungsvakuum ist weder mit den Zielen der Digitalisierungsstrategie des Bundes noch mit den Grundsätzen der Rechtssicherheit vereinbar.

Verschärft wird diese Problematik durch folgende Gesichtspunkte:

- Fehlende Verlängerungsmöglichkeit bestehender Zertifizierungen: Es ist nicht ersichtlich, wie Kantone, die den Übergang noch nicht vollzogen haben, eine Ausnahmeregelung beantragen könnten, um weiterhin auf bestehende zertifizierte Zustellplattformen zurückzugreifen. Mit dem Wegfall der bundesrechtlichen Zertifizierungsgrundlage entfällt auch die Möglichkeit kantonaler Eigenregelungen in diesem Bereich. Die ausschliessliche Lösung über Art. 6a Abs 4 VwVG mit der Abhängigkeit einer Einwilligung durch die Partei schafft eine erhebliche Regelungs- und Prozessunsicherheit und vermag für einen geordneten Rechtsverkehr keine Abhilfe zu schaffen.
- Auswirkungen auf die Verwaltungsverfahren: Die bisherige VeÜ-VwV-Zertifizierung wurde nicht nur für Gerichts-, sondern auch für Verwaltungsverfahren auf Bundes- und Kantonsebene genutzt. Diskussionen über eine neue einheitliche Plattform für Verwaltungsverfahren sind zwar im Gange, ein konkretes Konzept liegt jedoch noch nicht vor. Das Fehlen einer rechtlich anerkannten Zustelllösung wird insbesondere die Verwaltungsverfahren auf Bundesebene beeinträchtigen, wo IncaMail derzeit am weitesten verbreitet ist.
- Verweise in kantonalen Rechtsgrundlagen: Verschiedene Kantone – exemplarisch sei der Kanton Zürich mit dem VRG/VeVV genannt – verweisen in ihren eigenen Digitalisierungsgesetzen auf eine «bundesweit anerkannte digitale Zustellplattform» im Sinne der VeÜ-VwV-Zertifizierung. Tritt das VRG/VeVV zeitgleich mit dem BEKJ in Kraft, verweist es damit auf eine Grundlage, die zu diesem Zeitpunkt bereits ausser Kraft getreten ist.

Wir begrüssen, dass das Bedürfnis nach praktikablen Übergangslösungen grundsätzlich erkannt wurde. **Gleichwohl regen wir an, vor Ausserkraftsetzung des bestehenden Rechts systematisch zu prüfen, welche Verweise in Bundesverordnungen und kantonalen Erlassen auf die bisherigen Zertifizierungsregimes bestehen, und eine koordinierte Anschlussregelung zu schaffen.** Nur so kann ein kohärentes rechtliches Ökosystem sichergestellt und ein Regelungsvakuum mit negativen Folgen für die Rechtssicherheit vermieden werden.

2. Anschlussfähigkeit an BEKJ-Plattformen garantieren

a. Grundsätzliches

Das Primat der BEKJ-Plattformen für zwingend erfasste Verfahren wird durch die nachfolgenden Überlegungen nicht in Frage gestellt. Gleichzeitig ist festzuhalten, dass der Bedarf an vertrauenswürdiger elektronischer Zustellung deutlich über den Anwendungsbereich des BEKJ hinausgeht und auch privatrechtliche, wirtschaftliche sowie behördliche Kommunikation ausserhalb von entsprechenden Verfahren umfasst. Gerade für Nutzerinnen und Nutzer, die nicht dem Obligatorium zur Nutzung der BEKJ-Plattformen unterstehen, ist eine Anschlussfähigkeit zentral, da sie eine niederschwellige Einbindung ermöglicht und damit wesentlich zur breiten Akzeptanz und Nutzung der BEKJ-Plattformen beiträgt.
Um Kommunikationssilos zwischen unterschiedlichen Stakeholder-Gruppen (Behörden, Unternehmen, Private, Bevölkerung) sowie zwischen BEKJ-Plattformen und anderen digitalen Zustell- und Fachplattformen zu vermeiden, sollte die VEKJ daher ausdrücklich vorsehen, dass auch elektronische Sendungen der Post, einschliesslich des hybriden Zustellsystems, sowie entsprechende Dienste anderer Akteure als zugelassene elektronische Zustelldienste an Plattformen nach BEKJ angebunden werden können.

b. Anbindung zugelassener elektronischer Zustelldienste

Mit der Aufhebung der bisherigen Verordnungen (VeÜ-VwV und VeÜ-ZSSV) entfällt die rechtliche Grundlage für den Einsatz ehemals zertifizierter elektronischer Zustelldienste wie IncaMail im elektronischen Rechtsverkehr der Justiz. Der vom Bundesrat skizzierte Ansatz, wonach solche Dienste über Organisationsprofile und API-Token weiterhin in bestehende Abläufe eingebunden werden können, ist grundsätzlich zu begrüssen.
In der vorliegenden Ausgestaltung bleiben jedoch wesentliche Fragen offen zu den technischen und organisatorischen Anbindungen der ehemals zertifizierten Zustelldienste; den Rollen und Verantwortlichkeiten der beteiligten Akteure; den konkreten Schnittstellen und Prozesse nach Art. 19 BEKJ sowie der rechtlichen Behandlung, Übernahme und Protokollierung von Zustellnachweisen. Dies erschwert eine verlässliche Beurteilung der Praxistauglichkeit und schafft Unsicherheiten für alle Beteiligten.
Die Post regt daher an, die VEKJ um einen expliziten Zusatzartikel zu ergänzen, der klar regelt, unter welchen Voraussetzungen externe elektronische Zustelldienste an Plattformen nach BEKJ angebunden werden können und wie deren Zustellnachweise übernommen, validiert und protokolliert werden (siehe Formulierungsvorschlag nachfolgend in Abschnitt c). Ziel der vorgeschlagenen Anpassungen ist es, den bewährten qualitativen Standard, der durch die Umsetzung der VeÜ-VwV und VeÜ-ZSSV erreicht wurde, in das neue System der elektronischen Zustelldienste zu überführen und dabei die bestehende Systemlogik des BEKJ konsequent zu respektieren. Auf diese Weise kann Kontinuität im Vertrauens- und Qualitätsniveau gewährleistet werden, während gleichzeitig die angestrebte Systemvereinheitlichung unter dem BEKJ unterstützt wird. Eine solche Regelung unterstützt zudem bestehende Fachapplikationen und bewährte Prozesse, insbesondere für Kantone, vermeidet unnötige Systembrüche und fördert die Akzeptanz der BEKJ-Plattformen im praktischen Einsatz.

c. Einbindung des hybriden Zustellsystems

Die Postverordnung (VPG) verpflichtet die Post im Rahmen der Grundversorgung, elektronische Sendungen sicher, nachweisbar und anschlussfähig zu verarbeiten. Der elektronische Rechtsverkehr zählt als elektronische Sendung (Art. 1 lit. i & Art. 35a lit. f VPG). Der Digitale Brief ist dabei als hybrides Zustellsystem konzipiert, das elektronische und physische Zustellformen verbindet.
Vor diesem Hintergrund **sollte die VEKJ vorsehen, dass das hybride Zustellsystem der Post als zugelassener elektronischer Zustelldienst an Plattformen nach BEKJ angebunden werden kann.** Da es kein rein elektronischer Kanal ist, sollte dieses System sinnvollerweise als eigener, zugelassener Zustelldienst eingeordnet werden.
Eine solche Einbindung stärkt die BEKJ-Plattformen, indem sie deren Anschlussfähigkeit an Gesellschaft und Wirtschaft erhöht und bestehende, vertrauenswürdige Zustellinfrastrukturen in ein kohärentes und interoperables digitales Zustellökosystem integriert. Hier ein konkreter Formulierungsvorschlag:

Art. X VEKJ – Zugelassene elektronische Zustelldienste (neu)
1 Elektronische Zustelldienste sind zur Anbindung an Plattformen nach BEKJ zugelassen, sofern sie eine sichere, vertrauliche, nachweisbare und interoperable Übermittlung elektronischer Dokumente gewährleisten, die Zuordnung zu den übermittelten Dokumenten sicherstellen und die vom Bund festgelegten Anforderungen erfüllen.
2 Die Zulassung dient der Interoperabilität zwischen Plattformen nach BEKJ und externen Zustelldiensten; sie begründet keine Anerkennung als Plattform nach BEKJ und ersetzt die Nutzungspflicht nach BEKJ nicht.
3 Plattformen nach BEKJ können zugelassene elektronische Zustelldienste für die Übermittlung und den Empfang von Mitteilungen und Dokumenten zwischen obligatorischen Nutzerinnen und Nutzern nach BEKJ und nicht obligatorischen externen Nutzerinnen und Nutzern verwenden.
4 Zugelassene elektronische Zustelldienste können Zustell- und Übermittlungsnachweise sowie entsprechende Metadaten entgegennehmen, validieren, erzeugen und protokollieren. Diese Nachweise müssen den Zeitpunkt des Vorgangs sowie die Zuordnung zu den übermittelten Dokumenten nachvollziehbar und manipulationsgeschützt belegen.
5 Der Bund regelt die funktionalen, technischen und betrieblichen Anforderungen sowie die Schnittstellen und den Umgang mit Zustellnachweisen. Er kann insbesondere Anforderungen an die Verwendung von Zeitstempeln, elektronischen Siegeln, Zertifikaten, an die Verschlüsselung sowie an den Schutz vor unberechtigtem Zugriff festlegen.
6 Das hybride Zustellsystem der Schweizerischen Post nach der VPG wird als zugelassener elektronischer Zustelldienst angebunden, sofern es die Anforderungen nach Absatz 1 und 5 erfüllt.

Abschliessend erscheint auch eine Anpassung VPG erforderlich. Die VPG verweist heute direkt auf die bisherigen Verordnungen (VeÜ-VwV und VeÜ-ZSSV), welche im Zuge der Einführung des BEKJ und der VEKJ aufgehoben werden. Ohne entsprechende Anpassung entsteht eine systematische Inkonsistenz, da zentrale Bezugspunkte der VPG ihre Grundlage verlieren. Eine Aktualisierung ist daher notwendig, um die Anschlussfähigkeit an die neue Plattformarchitektur sicherzustellen, die Interoperabilität mit zugelassenen elektronischen Zustelldiensten zu gewährleisten und die kohärente Einbettung des hybriden Zustellsystems in den zukünftigen Rechtsrahmen zu sichern.
Vor diesem Hintergrund schlägt die Post folgende Präzisierung vor:

Art. 35a Bst. f VPG
1 Die Post stellt die Teilnahme am elektronischen Rechtsverkehr sicher. Elektronische Sendungen des Rechtsverkehrs müssen an Plattformen nach dem BEKJ und der VEKJ übermittelt und von solchen angenommen werden können.

3. Allgemeine Wirkung des Elektronischen Einschreiben erhalten

Die rechtliche Wirkung des eingeschriebenen Briefs beruht im schweizerischen Rechtsverkehr auf dem Zusammenspiel der Postverordnung (Art. 29 VPG), Rechtsprechung sowie den Grundsätzen der Empfangstheorie und Zustellfiktion. Diese Grundsätze gelten unabhängig vom Kommunikationsmittel und bilden die Grundlage für eine verlässliche rechtsverbindliche Zustellung.
Elektronische Einschreiben haben diese Funktion in der Praxis bereits übernommen. Insbesondere Aufgabe- und Abrufbestätigungen ermöglichen einen nachvollziehbaren Zustellnachweis und tragen zur Gleichwertigkeit von physischer und elektronischer Zustellung bei. Dadurch hat sich das Elektronische Einschreiben als etabliertes und verlässliches Instrument entwickelt, das heute eine wichtige Funktion im wirtschaftlichen und rechtlichen Gefüge der Schweiz erfüllt.

Mit der Aufhebung der bisherigen Zertifizierungsverordnungen besteht aus Sicht der Post die berechtigte Vermutung, dass Nutzerinnen und Nutzer die rechtliche Wirkung solcher Zustellnachweise vermehrt hinterfragen werden. Hintergrund ist, dass mit dem Wegfall der formellen Zertifizierungsgrundlage auch die bislang implizit anerkannte Verbindung zwischen Zustellnachweis und Empfangsbestätigung entfällt, was zu Unsicherheiten hinsichtlich der Anwendung der Empfangstheorie im digitalen Kontext führen kann. Eine solche Entwicklung könnte sich negativ auf das Vertrauen in elektronische Zustellungen auswirken und eine Rückverlagerung hin zu physischen Zustellformen begünstigen. Vor diesem Hintergrund ist es wesentlich, die bestehende Vertrauensbasis der Nutzerinnen und Nutzer in digitale Zustellmechanismen zu sichern.

Die Post regt daher an, in der Postverordnung klarzustellen, dass für elektronische Sendungen dieselben Grundsätze der Empfangstheorie gelten wie für physische eingeschriebene Sendungen. Dabei sollen bestehende technische Zustellnachweise des hybriden Zustellsystems (Abruf- und Nichtabrufbestätigungen - Art. 35b Abs. 4 VPG) als rechtlich massgebliche Zugangstatbestände anerkannt werden.

Eine solche Klarstellung stärkt die Rechtssicherheit, erleichtert die praktische Anwendung und gewährleistet, dass elektronische Zustellungen im allgemeinen Postverkehr denselben funktionalen Stellenwert behalten wie die physische Zustellung.

> *Art. 29 Abs. 3ter VPG (neu)*
> *1 Bei elektronischen Sendungen gilt eine Sendung als empfangen, wenn die Empfängerin oder der Empfänger, die ihr oder ihm zugestellte Sendung erstmals über den elektronischen Kanal abruft.*
> *2 Wird eine elektronische Sendung bis zum Ablauf des siebten Tages nach der Zustellung nicht abgerufen, stellt die Post eine Nichtabrufbestätigung aus; die Sendung gilt im Zeitpunkt der Ausstellung dieser Bestätigung als empfangen, sofern die Empfängerin oder der Empfänger mit einer Zustellung rechnen musste.*
> *3 Der Empfang ist durch eine geeignete elektronische Bestätigung nachzuweisen, welche insbesondere den Zeitpunkt der Zustellung, des Abrufs oder des Fristablaufs sowie die beteiligten Parteien dokumentiert.*

Wir bedanken uns für Ihre Kenntnisnahme und bitten Sie, die Vorlage entsprechend unseren Vorschlägen anzupassen. Für Fragen stehen wir Ihnen jederzeit zur Verfügung.

Freundliche Grüsse

Die Schweizerische Post AG

Matthias Dietrich
Leiter Stab CEO

Post CH Digital Services AG

Tecla Solari
Business Unit Head Trusted Interaction Services
Mitglied der Geschäftsleitung Digital Services
Verwaltungsratspräsidentin Tresorit

SSK | CMP
Schweizerische Staatsanwaltschaftskonferenz SSK
Conférence suisse des Ministères publics CMP
Conferenza svizzera dei Ministeri pubblici CMP

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundesamt für Justiz

Per E-Mail: cornelia.perler@bj.admin.ch

Bern, 20. Mai 2026

Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 13. März 2026 haben Sie unsere Konferenz eingeladen, an obgenannter Vernehmlassung teilzunehmen. Dafür danken wir Ihnen bestens.
Die SSK konzentriert sich in ihrer Stellungnahme auf jene Punkte im aktuellen Entwurf der Verordnung (nachfolgend Entwurf), die für die Staatsanwaltschaften von zentraler Bedeutung sind. Dies sind aus Sicht der SSK folgende 12 Punkte:

1. Technische Spezifikation

Der Entwurf legt u.a. in den Artikeln 2,4, 14 und 22 zahlreiche technische Spezifikationen fest, namentlich Dateigrösse, abschliessender Datei-Format-Katalog, Datei-Grössen-Begrenzung/Aufteilung für Virenprüfung und Farbtiefe/Auflösung.

Die zeitliche Dynamik sowie die Entwicklungsgeschwindigkeit im Berich der Informatik steht in keinem Verhältnis zur durchschnittlichen Dauer eines Gesetzgebungsverfahrens, sei es auf Stufe Gesetz aber auch Verordnung. Mit der in der Regel zurückhaltenden Legiferierung von heute geltenden technischen Standards in der Verordnung riskiert man, dass diese bereits bei Inkrafttreten der Verordnung überholt sind. Anpassungen sind aufwändig und in der Regel nicht zeitnah umsetzbar. Im Rahmen der Revision der Verordnungen im Bereich der Fernmeldeüberwachung zeigte sich, dass wegen der Legiferierung von technischen Spezifikationen einer Applikation gewisse Funktionalitäten der Nachfolge-Version nicht genutzt werden durften.
Mit Bezug auf technische Angaben müssen deshalb **Lessons learned** aus anderen Regelungsbereichen auch in diesen Gesetzgebungsprozess einfliessen: Dateigrösse, Datei-Grössen-Begrenzung/Aufteilung für Virenprüfung und Farbtiefe/Auflösung etc. gehören nicht in die Verordnung, sondern sollten in der Departements-Verordnung aufgenommen oder noch besser **in einem Anhang zum VEKJ.** Die Verordnung über die technischen Anforderungen an Strassenfahrzeuge (SR 741.41) zum Beispiel enthält nicht weniger als 14 Anhänge, worin die jeweils schnelllebigen technischen Entwicklungen laufend und einfach angepasst werden können.

Grundsätzlich begrüssen wir die Beschränkung auf wesentliche Formate, falls möglich und sinnvoll. Aus praktikablen Gründen ist PDF für viele Dokumente ein geeignetes Format. Deshalb sollte das Format PDF,

anders als im Entwurf vorgesehen, auch als das Standardformat für Beilagen vorgesehen werden. Wo also etwa einige Bilder oder eine Excel-Tabelle gut in ein PDF-Dokument konvertiert werden können, sollte dies auch geschehen, um die sog. «Veraktung» bei den verfahrensleitenden Behörden zu vereinfachen. Auf die Umformung sollte nur dort verzichtet werden, wo Informationen verloren gehen, die für das Verfahren wesentlich sind, Primärdaten unerlässlich und deren Bearbeitung notwendig ist.

Abs. 2 von Art. 4 der Verordnung sollte deshalb lauten: *«Ist das Format PDF ungeeignet, den Inhalt eines Dokuments korrekt wiederzugeben oder sind Primärdaten erforderlich, kann die Beilage im Originalformat übermittelt werden.»*

2. Definition der «Behörde»

Es stellt sich die Frage nach dem persönlichen Geltungsbereich des BEKJ bzw. der VEKJ. Vor allem der Begriff «Behörde» ist unklar. Es besteht eine Unsicherheit, welche üblicherweise von der Staatsanwaltschaft beauftragten «Behörden» die Plattform verwenden müssen, um sich an die Staatsanwaltschaft zu wenden.

Ist zum Beispiel das Institut für Rechtsmedizin eine Behörde? Wie verhält es sich mit Psychiatrien oder einer öffentlich-rechtlichen Transportunternehmung? Im Kanton Zürich ist das Institut für Rechtsmedizin eine öffentlich-rechtliche Anstalt und ein Institut der Universität Zürich. Das Forensische Institut wiederum ist eine selbständige öffentlich-rechtliche Anstalt. Diverse Busbetriebe werden von Gemeinden betrieben.

Zudem fällt auf, dass der Regelungsbereich von Art. 103*c* nStPO den «Austausch von Dokumenten *mit der Strafbehörde*» umfasst. Art. 24 VEKJ, der sich u.a. genau auf diese Bestimmung der nStPO stützen will, führt aber allgemeine Sonderregelungen für den Rechtsverkehr von «Behörden untereinander» ein.

Wenn in den Erläuterungen zu Art. 24 VEKJ davon die Rede ist, auch der Rechtsverkehr zu Gerichten könne etwa «ausserhalb einer Plattform nach dem BEKJ» erfolgen, entsteht ein Widerspruch zum insoweit klaren Wortlaut von Art. 103*c* nStPO und das Verhältnis zur Sonderregelung unter Strafbehörden in Art. 103*b* nStPO kann nicht mehr erklärt werden.

Aus den Erläuterungen zu Art. 24 VEKJ folgt, dass «Amtsstellen» unter den Begriff der Behörde fallen. Ob dies auf ein Busunternehmen eines Kantons zutrifft, ist fraglich und offen. Diesbezüglich ist der Entwurf zu konkretisieren und **der persönliche Geltungsbereich explizit zu regeln[1].**

3. Definition der «Partei»

Die VEKJ enthält keine auslegende Bestimmung zu Art. 103*d* nStPO. Dies wäre jedoch notwendig, weil sich aus dem Titel und dem ersten Absatz ein Widerspruch ergibt. Während im Titel und auch in der Kommentierung zu Art. 11*b* Abs. 2 E-VWVG (Botschaft BEKJ, BBl 2023 679, S. 44 von «Parteien» die Rede ist, spricht Art. 103d Abs. 1 nStPO von «Person». Trifft dies auch für juristische Personen zu, die regelmässig mit den Strafbehörden Dokumente austauschen müssen (Bspw. bei Editionsaufforderungen)?

Aus Sicht der SSK muss klargestellt werden, ob unter «Person» auch juristische Personen des Privatrechts zu subsumieren sind und diese die Plattform zum elektronischen Rechtsverkehr mit den Strafbehörden auch dann nutzen dürfen, wenn sie keine Parteistellung im Verfahren haben.

[1] Zum Parallelproblem der obligatorischen Siegelung von Dokumenten, die nach hier vertretener Ansicht nur die verfahrensleitenden Behörden treffen sollte, vgl. Ziff. 4 unten.

4. Umgang mit Fristen

Gemäss Art. 22 Abs. 4 lit. b BEKJ erstellt die Plattform im Moment des Abrufs einer Sendung eine Abrufquittung aus. Damit werden allfällige Fristen ausgelöst. Je nach Organisation einer Behörde kann eine Frist durch die empfangende Person ausgelöst werden, obwohl es sich hierbei nicht um den Adressaten handelt. Im Innenverhältnis der Behörde kann die Feinverteilung der Sendungen Zeit in Anspruch nehmen oder es wird erst später festgestellt, dass der Adressat nicht anwesend ist.

Die Gewährleistung der internen Zustellung ist primär Sache der Staatsanwaltschaften. Stellvertretungen sind zu regeln und die Informationswege zu gewährleisten. Zudem wird die zukünftige Anbindung der Plattform an eine Fachanbindung mittels einer Schnittstelle Lösungen bringen.

Zwischenzeitlich haben aber Pilotkantone dieses Problem festgestellt und «überbrücken» das Problem der Fristauslösung bei Entgegennahme ausserhalb der Bürozeiten mit Ausweichen auf alternative Zustellplattformen.

Solange die Fachapplikationen noch nicht mit Schnittstellen an die Plattform angebunden sind und die Weiterleitung an die zuständige Person noch nicht gewährleisten können, sollte die Plattform nur von Personen bedient werden, die mit ihrer Handhabung vertraut sind. Dies, um zu vermeiden, dass irrtümlich Fristen in Fällen anderer Fallbearbeiter ausgelöst werden, exemplarisch und besonders heikel bei Haftentlassungsgesuchen. Mit Wegfall der VeÜ-ZSSV wird allerdings die Verwendung von IncaMail etc. nicht mehr möglich sein, während die Fachapplikationsanbindung (und damit die Feinverteilung) vielerorts noch nicht gewährleistet ist. Die Möglichkeit zur Weiterverwendung von IncaMail, etc. während einer Übergangszeit würde dieses Problem verringern.

5. Siegelung

Im Gegensatz zu einer (qualifizierten) digitalen Signatur (QES), die stets einem authentifizierten Benutzer zuzuordnen ist, gibt ein Siegel nur Auskunft über die das Dokument erlassende Behörde. Art. 22 Abs. 2 BEKJ sowie der Art. 6 des Entwurfs verlangen entgegen den gegenwärtigen Bestimmungen nach VeÜ-ZSSV sowie Zert-ES keine QES mehr, sondern lassen ein Siegel als Nachweis der durch eine Behörde autorisierte Ausstellung eines Dokuments genügen.

Zunächst ist festzustellen, dass die Ausführungen im erläuternden Bericht des Bundesamtes für Justiz vom 13. März 2026 (Erläuterungen zu Art. 6 VE-VEKJ, S. 18), wonach eine Behörde alle Dokumente mit einem Siegel versehen muss, dem Wortlaut von Art. 6 des Entwurfs widersprechen.

Durch eine zu weite Auslegung von Art. 22 Abs. 2 BEKJ könnten *sämtliche* Behörden zur Siegelung allfälliger Eingaben an die Strafbehörden gezwungen werden (bspw. die Steuerverwaltung, wenn sie der Staatsanwaltschaft Auskunft über die finanziellen Verhältnisse einer Person erteilt).

Gemäss gegenwärtiger Rechtsprechung müssen gewisse Dokumente eine Unterschrift der Autorenschaft tragen, namentlich Sachverständigengutachten (BSK StPO-Heer, Art. 187 N 1). Diese können etwa im Fall von rechtsmedizinischen Instituten oder im Fall des Eidgenössischen Instituts für Metrologie METAS durchaus auch von Behörden oder zumindest von “Amtsstellen” erbracht werden. In diesen Fällen ist es erheblich, welche sachverständige Person das Gutachten erstattet, weshalb die qualifizierte elektronische Signatur (entgegen der Kommentierung zu Art. 22 BEKJ in der Botschaft, BBl 2023 679 ff., S. 30) im Bereich der elektronischen und rechtsgültigen Übermittlung von Dokumenten unerlässlich scheint.

Anders als bei der Anwaltschaft wird etwa im Fall eines Instituts für Rechtsmedizin kaum jede sachverständige Person über ein eigenes Profil auf der Plattform verfügen, mit dem die Urheberschaft von Eingaben eindeutig zu klären wäre.

Haltung SSK:

Wir sind entschieden der Ansicht, dass die Siegelungspflicht nur die verfahrensleitenden Behörden treffen kann. Zusätzlich wäre aber eine Klärung der Erforderlichkeit der qualifizierten elektronischen Unterschrift aller anderen Verfahrensbeteiligten zu begrüssen.

Zum Problemkreis der Anzahl der zu siegelnden Dokumente vertreten wir die Auffassung, dass grundsätzlich die Siegelung eines Dokuments durch die verfahrensleitende Behörde genügt.

Zum Problem der gesetzlichen Erforderlichkeit der Unterzeichnung des Verfassers eines Dokuments im Sinne der genannten Beispiele ist zu klären, inwieweit die Erkennbarkeit des Ausstellers ausreicht. Sollte daneben auch die Unveränderbarkeit eines Dokuments nach der Fertigstellung durch die Autorin oder den Autor erforderlich sein, wovon nach der hier vertretenen Meinung auszugehen ist, wäre eine (qualifizierte) digitale Signatur zwingend.

6. Quittungen

Träger des Siegels der Plattform ist immer die Quittung, nie das übermittelte Dokument. Im Fall der zentralen Plattform handelt es sich beim separaten Dokument gemäss Art. 7 Abs. 1 des Entwurfs um die Eingangs-, Abruf- oder die Nichtabholquittung.

Scheitert die Übermittlung aus technischen Gründen, ist dies nicht ersichtlich. Nicht übermittelte Dokumente können nicht ausgewiesen werden. Hier wurde an den technischen Limiten vorbei legiferiert.

Neben Dokumenten lässt die Plattform die Übermittlung von strukturierten Daten im XML-Format zu (Bspw. Aktenstruktur von Dokumenten). Die Funktionalität dieser Dateiformate wird durch Siegel allfällig negativ beeinträchtigt.

Haltung SSK:
Zu unterscheiden sind die Siegelung von Dokumenten durch die erstellende Behörde und die Siegelung der Übermittlungsergebnisse durch die Plattform. Unseres Erachtens vermischt der erläuternde Bericht zwei verschiedene Aspekte, nämlich die unveränderbare Quittierung der elektronischen Kommunikation über die Plattform und die Siegelung von Dokumenten durch die jeweilige Behörde.

Die Plattform weist auf der Quittung die Metadaten der Übermittlung, des Absenders und des Inhalts der Sendung aus (Art. 5 Abs. 2 lit. a bis g des Entwurfs). Diese Angaben werden mit dem Siegel und dem Zeitstempel unveränderbar gemacht.

Demgegenüber muss ein Dokument, welches eine Behörde übermittelt, gesiegelt werden, damit die Authentizität des Dokuments unabhängig von der Plattform geprüft werden kann.

Diese zwei Regelungsziele sind klar zu unterscheiden.

Sodann muss die Plattform strukturierte Daten übermitteln können, beispielsweise in Form von XML-Dateien. Die Ausnahmen in den Absätzen 4 und 5 sind daher wesentlich, da XML-Dateien aus technischen Gründen nicht gesiegelt werden können.

Schliesslich ist festzuhalten, dass es technisch nicht möglich ist, über nicht übermittelte Dokumente eine Quittung auszustellen. Allfällig lässt sich eine Fehlermeldung über eine nicht vollständige oder nicht korrekte Übermittlung eines oder mehrere Dokumente auf der Quittung darstellen.

7. Aufbewahrung Dokumente und Quittungen

Bei dieser Regelung geht es um eine Abwägung von Strafverfolgungs- mit Datenschutzinteressen. Die Plattform soll keine Langzeitablage sein, dennoch können Quittungen sehr spät im Verfahren noch benötigt

werden, um etwa die Einhaltung einer Frist oder die Kenntnisnahme eines bestimmten Dokuments zu belegen.

Unter diesem Aspekt ist es gerade bei den Quittungen angezeigt, eine längere Aufbewahrungsfrist vorzusehen. Art. 12 des Entwurfs sieht vor, neben den hochgeladenen Dokumenten auch Quittungen nach Ablauf einer Frist von sechs Monaten nach ihrer Erstellung auf der Plattform automatisch zu vernichten.

Die automatisierte Löschung von Zustellungen und Eingaben nach einer überschaubaren Zeitspanne ist zu begrüssen. Die Plattform soll ein «Briefkasten» und keine Langzeitablage sein. Der Umfang von zu speichernden Dokumenten birgt vermeidbare Sicherheits- und Datenschutzrisiken und würde auch immense Kosten für die benötigte Infrastruktur verursachen. Daher ist eine Frist von sechs Monaten angemessen.

Haltung SSK:
Bei Quittungen verhält es sich, wie ausgeführt, anders. Natürlich müssen die Behörden darum besorgt sein, die Quittungen in ihre eigenen Umgebungen und in die Akten zu überführen. Im Falle von Unterlassungen der Ablage oder Bedarf an Daten aus der Primärquelle erscheint bei den Quittungen eine längere Aufbewahrungsfrist angezeigt: Wir schlagen eine Verlängerung der Aufbewahrungsfrist für Quittungen auf drei Jahre vor. Dies würde der Frist entsprechen, welche die Post für Nachforschungsaufträge kennt.

8. Rücksendung von Dokumenten

Ziffer 2.6 des erläuternden Berichts (S. 7) legt dar, es sei darauf verzichtet worden, eine Bestimmung zur reduzierenden Auslegung von Art. 30 BEKJ in die Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren der Verordnung aufzunehmen, weil hierfür kein gesetzlicher Handlungsspielraum verbleibe. Diese Feststellung bezieht sich auf die Auslegung des in Art. 30 BEKJ enthaltenen Begriffs der «Dokumente», der im Gesetz weder weiter nach Rechtsgebiet noch nach Dokumentinhalt unterschieden wird.

Eine differenzierende Betrachtung ist aber erforderlich, da eine lückenhafte Verordnung zum BEKJ Probleme schafft, die es in der analogen Welt und heute gar noch nicht gibt:

Im Strafprozess werden physisch eingereichte Dokumente nur in Ausnahmefällen an deren Absenderin oder Absender retourniert. Bei den Polizeikorps und den Staatsanwaltschaften werden auch nach der Inkraftsetzung der Änderungen der massgebenden Verfahrensgesetze noch jährlich tausende von Anzeigen etc. in Papierform eingehen, da solche Eingaben typischerweise von Privatpersonen stammen, die sich nicht zuerst auf der Plattform «justitia.swiss» registrieren wollen.

Diese grosse Menge an Eingaben wird für die Strafbehörden geschrieben und in der Regel mit Kopiensätzen an Beilagen ergänzt. Die Quelle oder das Original verbleibt in beiden Fällen bei der Absenderin oder dem Absender.

Wird das BEKJ nicht reduzierend ausgelegt, wofür gemäss den Erläuterungen zum vorliegenden Vorentwurf kein Raum bestehen soll, werden mit einem Gesetz, mit dem der elektronische Rechtsverkehr eingeführt werden soll, neue Rücksendungspflichten im Papierprozess eingeführt, die bisher nicht existierten. Dies kann nicht der Willen des Gesetzgebers gewesen sein.

Der Rückversand von Schriftstücken entfaltet keinerlei Nutzen, wenn sich der Zweck eines Dokuments in der Weitergabe der Mitteilung erschöpft. Die Absenderinnen und Absender solcher Mitteilungen verfügen bereits über Doppel ihrer Eingaben oder über die Originale, von denen sie Fotokopien angefertigt haben. Die zurückgeschickten Exemplare werden bestenfalls entsorgt.

Auch für den eher gesuchten Fall, dass im Nachhinein Differenzen darüber entstünden, ob die digitalisierten Kopien in den behördlichen Akten den eingereichten Dokumenten entsprechen, kann mangels eines Belegs über die Unveränderbarkeit nicht Beweis geführt werden, ob kongruente Dokumente eingereicht worden sind.

Diese durch eine zu enge Auslegung des BEKJ verstandene Rücksendepflicht in Papierform würde einen enormen Mehraufwand durch Porti und Versandarbeit schaffen.

Haltung SSK:
Der Unterschied zwischen einfachen Mitteilungen und Dokumenten, denen neben dem Mitteilungsinhalt noch zusätzlicher Gehalt zukommt, ist bereits im BEKJ angelegt. Art. 30 Abs. 2 BEKJ sieht vor, Dokumente bei den Behörden zurückzubehalten, wenn sie im Verfahren noch benötigt werden. Dies trifft auf sämtliche Dokumente zu, die forensisch gesicherte Spuren enthalten oder enthalten könnten, namentlich handschriftliche Unterschriften, Siegel, Fingerabdrücke, DNA-Spuren oder chemische Rückstände von Substanzen.

Überdies geht aus der Botschaft zum Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz vom 15. Februar 2023 (BBl 2023 679 ff.) hervor, dass Dokumente, denen Urkundencharakter zukommt, nicht unmittelbar zurückgesandt werden sollen (Erläuterungen zu Art. 30 E-BEKJ, S. 36 der Vorlage).

E contrario könnte daraus geschlossen werden, dass bei allen anderen Dokumenten keine Rücksendepflicht besteht.

Um aber nicht auf die Auslegung einer allfälligen gesetzgeberischen Lücke angewiesen zu sein, schlagen wir einen neuen Artikel 22a vor, dessen Formulierung klarstellt, dass Dokumente, die gemäss Artikel 30 Absatz 2 BEKJ zurückbehalten werden, nicht von der Rücksendepflicht befreit sind. Trifft allerdings eines der danach genannten alternativen Kriterien zu, kann von einer Rücksendung abgesehen werden.

Durch diese Ergänzung würde dem gesetzgeberischen Normzweck durch eine Negativauslegung des Dokumentenbegriffs gemäss Artikel 30 BEKJ Rechnung getragen. Sollte die Absenderin oder der Absender dennoch ein Interesse an einem Rückversand haben, kann sie oder er diesen vorab verlangen.

Für Art. 22a schlagen wir folgenden Text vor:
[...]
Art. 22a Rücksendung von physischen Dokumenten
Ohne vorgängiges, anderslautendes Ersuchen der Absenderin oder des Absenders sind Aktenstücke von der Pflicht zur Rücksendung physisch eingereichter Dokumente gemäss Artikel 30 Absatz 1 BEKJ ausgenommen, wenn sie nicht unter Artikel 30 Absatz 2 BEKJ fallen und wenn sie gemäss dem anwendbaren Prozessrecht nicht handschriftlich unterzeichnet werden müssen oder wenn ihnen in elektronisch eingelesener Form derselbe Beweiswert zukommt, namentlich Ausdrucke elektronisch erstellter Dokumente oder Fotokopien.

9. Trägerwandel

Gemäss Ziffer 2.6 des erläuternden Berichts wurde die Idee, die Eröffnung elektronisch unterzeichneter Endentscheide durch einen Versand von Papierkopien sicherzustellen, verworfen, weil die anwendbaren Gesetzesbestimmungen hierfür keinen Raum liessen. Konkret geht es dabei darum, dass etwa Artikel 353 Absatz 1 Buchstabe k nStPO für das Strafbefehlsverfahren der Staatsanwaltschaften vorschreibt: «Der Strafbefehl enthält: (...) die Unterschrift der ausstellenden Person, falls der Strafbefehl auf Papier versendet wird.»

Artikel 22 konkretisiert Art 29 BEKJ und damit den Trägerwandel von der Papiereingabe zum elektronischen Aktenstück.

Der umgekehrte Vorgang wird im BEKJ jedoch nicht beschrieben, obwohl es sich dabei in der Praxis um eine sehr gewichtige Anforderung handeln würde, denn Standard soll gemäss dem Grundkonzept des BEKJ die elektronische Aktenerstellung sein. Wo sich Private aber nicht auf einer elektronischen Übermittlungsplattform registrieren wollen, haben sie auch inskünftig das Recht, dass ihnen ein Papierexemplar von Mitteilungen und Entscheiden zugestellt wird. Daher wird eine Vielzahl von Trägerwandeln anstehen, zum Beispiel und insbesondere bei den Übertretungsstrafbehörden.

Wie oben ausgeführt, stellt zukünftig ein geregeltes elektronisches Siegel sicher, ob ein elektronisch erstelltes Dokument tatsächlich der zuständigen und bspw. aus dem Briefkopf erkennbaren Behörde stammt. Zu diesem Artikel ist der Botschaft zum BEKJ zu entnehmen: «Das Unterschriftserfordernis stellt bei der Digitalisierung oft ein Hindernis dar. Anstelle der Unterschrift sieht das Gesetz die Authentifizierung mit Hilfe eines anerkannten elektronischen Identitätsnachweises sowie dem Anbringen eines geregelten elektronischen Siegels vor.» (Botschaft zum Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz vom 15. Februar 2023 (BBl 2023 679 ff., Vorbemerkungen zu Art. 22, S. 30 der Vorlage).

Daraus folgt, dass das geregelte elektronische Siegel bei einer elektronischen Aktenführung die Papierunterschrift ersetzt. Für einen Rückgriff auf Artikel 14 OR[2] bleibt damit im Anwendungsbereich des BEKJ kein Raum mehr. Das BEKJ als das jüngere und speziellere Gesetz ersetzt die eigenhändige Unterschrift von Behördenmitgliedern durch ein geregeltes elektronisches Siegel (zum Schutzniveau vgl. die Botschaft, a.a.O., zu Art. 22 BEKJ).

Dies ist doch recht bemerkenswert, zumal auch der aktuelle Art. 353 Abs. 1 lit. k StPO die Unterschrift der ausstellenden Person noch verlangt und erst im Zuge der Inkraftsetzung der diesbezüglichen Bestimmungen des BEKJ angepasst wird. Inskünftig braucht es die handschriftliche Signatur nur noch, wenn das Original eines Strafbefehls in Papierform erstellt wird.

Damit wird klar, wohin die Reise gehen soll. Der gesetzgeberische Wille hin zum digitalen Fortschritt soll daher nicht durch eine restriktive Auslegung des Unterschriftserfordernisses verhindert werden.

Haltung SSK:
Aus dem erläuternden Bericht geht hervor, dass gemäss den Verfahrensgesetzen etwa Endentscheide die Unterschrift der ausstellenden Person tragen müssen, wenn sie als Original in Papierform versandt werden. Bei Trägerwandel darauf zu beharren, entspräche einer zu engen Auslegung im Sinne des offensichtlichen und eindeutigen Gesetzeszweckes.

Bereits heute ist es absolut gängige Praxis bei den Strafbehörden, das Original der Endentscheide zu den Akten zu nehmen und den Parteien eine Fotokopie des Originals zuzustellen.

Wie beim Rückversand sollen auch hier keine neuen Pflichten, sondern Vereinfachungen geschaffen werden. Die gemäss erläuterndem Bericht verlangte Pflicht zum Versand eines Papieroriginals ist nicht zielführend.

---

[2] **Art. 14 OR Unterschrift**
[1] Die Unterschrift ist eigenhändig zu schreiben.
[2] Eine Nachbildung der eigenhändigen Schrift auf mechanischem Wege wird nur da als genügend anerkannt, wo deren Gebrauch im Verkehr üblich ist, insbesondere wo es sich um die Unterschrift auf Wertpapieren handelt, die in grosser Zahl ausgegeben werden.
[2bis] Der eigenhändigen Unterschrift gleichgestellt ist die mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur gemäss Bundesgesetz vom 18. März 2016[4] über die elektronische Signatur. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.[5]
[3] Für den Blinden ist die Unterschrift nur dann verbindlich, wenn sie beglaubigt ist, oder wenn nachgewiesen wird, dass er zur Zeit der Unterzeichnung den Inhalt der Urkunde gekannt hat.

Vielmehr muss klargestellt werden, worum es sich bei der postalischen Zustellung einer Verfügung handelt. Es kann und darf nicht mehr sein als eine Notifikation gegenüber einer nicht auf der Plattform registrierten Person darüber, dass ein elektronisches Original vorliegt (in Deutschland wird dafür der Begriff der **«Urschrift»** verwendet).

Der Papierkopie kommt exakt derselbe Informationsgehalt zu wie dem elektronischen Original. Dafür braucht es keine handschriftliche Signatur. An dieser Stelle sei auf die schiere Menge an Strafbefehlen hingewiesen, welche die Staatsanwaltschaften jährlich ausstellen: Bei der Staatsanwaltschaft des Kantons Aargau zum Beispiel waren dies im Jahr 2025 41'907, bei der Staatsanwaltschaft des Kantons Luzern 46'145 und bei der Staatsanwaltschaft des Kantons St. Gallen 48'485. Sollte die Empfängerin oder der Empfänger Zweifel an der Urheberschaft des Entscheids hegen, könnte sie oder er sich jederzeit das elektronische Original zustellen oder sich dieses am Sitz der Behörde zeigen lassen.

In formaler Hinsicht ist auch einzuwenden, dass per definitionem eine Kopie kongruent mit dem Original zu sein hat. Wird die Papierkopie des elektronischen Originals mit einer handschriftlichen Unterschrift verändert, handelt es sich streng genommen nicht mehr um eine Kopie, sondern um ein anderes Dokument.

Insofern verhindert die vorgeschlagene Lösung auch in formaler Hinsicht, dass in einem Verfahren plötzlich zwei nicht eindeutig kongruente «Originale» desselben Entscheids nebeneinander bestehen (etwa dann, wenn eine beschuldigte Person verteidigt ist und ihr somit über ihre Rechtsvertretung ein elektronisch gesiegeltes Exemplar des Endentscheids (ohne jegliche Unterschrift) zugesandt werden dürfte, während die Privatklägerschaft nicht anwaltlich vertreten ist und ihr eine Papierkopie zugeschickt werden müsste, die dann wiederum eine von Hand angebrachte Unterschrift tragen müsste). Zudem ergäbe sich auch eine identische Rechtslage zur Bundesgerichtsbarkeit. Das nBGG sieht für Urteile gerade nicht vor, dass diese im Fall ihres Papierversands eine Unterschrift tragen müssen.

Wir schlagen deshalb vor, einen neuen Artikel 22b mit folgendem Wortlaut im Entwurf einzufügen:

Art. 22b Zustellung von Papierkopien von elektronisch erzeugten Originaldokumenten
Behörden, die ihre Akten elektronisch führen, bringen auf Dokumenten, für die das anwendbare Verfahrensrecht für deren Papierform die Unterschrift mindestens einer Behördenvertretung vorsieht, ein geregeltes elektronisches Siegel an, wenn sie diese Dokumente versenden müssen. Soweit derlei Dokumente (auch) Personen eröffnet werden müssen, mit denen die Behörde nicht elektronisch verkehrt, erfolgt die Übermittlung des Dokuments mittels einer Papierkopie des elektronischen Originals. Die Zustellung der Papierkopie wirkt fristauslösend, wenn die angeschriebenen Personen auf der Papierkopie darauf hingewiesen werden, dass sie das elektronische Original kostenlos über eine Plattform nach BEKJ beziehen oder bei der Behörde ein von Hand unterschriebenes Doppel nachverlangen können.

Dieser Ansatz ist folgelogisch und deckt sich mit dem Paradigmenwechsel hin zum elektronischen Original eines Dokuments. Sollte an der viel zu engen Auslegung des BEKJ im erläuternden Bericht festgehalten werden, ist zumindest der Einsatz einer qualifizierten elektronischen Unterschrift der Behördenmitglieder (zusätzlich zum Behördensiegel) zu prüfen. Die QES lässt sich schon heute mit dem in den Verfahrensgesetzen verwendetem Begriff der «Unterschrift» gleichsetzen, obwohl sich diese, wie weiter oben ausgeführt, im Kontext der digitalen Aktenführung überwiegend durch das Behördensiegel ersetzen liesse.

Obligatorium und Ausnahmen

Art. 23 VE-VEKJ konkretisiert u.a. Artikel 103b Absatz 2 StPO. Es ist davon auszugehen, dass sich diese Bestimmung an die Kommunikation zwischen Strafbehörden innerhalb der Strafprozesskette richtet, bei der Akten beispielsweise bei einem Weiterzug an die übergeordnete Instanz weitergegeben werden

müssen, wo andere Behörden mit bestimmten Verfahrenshandlungen beauftragt werden (Bsp. Ermittlungsauftrag von Staatsanwaltschaft an die Kriminalpolizei) oder bei der Übermittlung von Ergebnissen von Untersuchungshandlungen, welche die Polizei an die Staatsanwaltschaft übermittelt.

Die vorgeschlagenen Ausführungsbestimmungen orientieren sich stark an der technischen Lösung der Plattform. Bei der elektronischen Weitergabe unter Strafbehörden sollten jedoch andere Anforderungen gelten als bei der Kommunikation über die Plattform.

Ein weiterer Problemkreis liegt in der Formulierung von Art. 24 VE-VEKJ. Unseres Erachtens ist die Sachüberschrift von Art. 24 des Entwurfs zu weit gefasst und daher irreführend. Im strafprozessualen Kontext handelt es sich stets um die Kommunikation von und zu Strafbehörden im Rahmen von Verfahren nach StPO. Gleichzeitig erscheint es erforderlich, den Begriff der übrigen Behörden - also jene, die unter das Obligatorium fallen, mit den Strafbehörden elektronisch zu kommunizieren - zu definieren (vgl. oben Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.**) und die nötige Klarheit zu schaffen.

Haltung SSK:
Wir sind klar der Ansicht, dass grundsätzlich der elektronische Rechtsverkehr über die Plattform abgewickelt werden soll. Gewisse Ausnahmen sind aber denkbar. Allen voran bei etablierten Schnittstellen zwischen Fachapplikationen. Oder aber auch bei einer Vielzahl von Schriftwechseln mit Behörden, die nicht Teil der Straf- oder Zivilprozesskette sind, wo keine Schnittstelle besteht oder aus Kostengründen dem Rechtsverkehr über die Plattform vorgezogen wird.

Zu denken ist im Strafprozess etwa an Steuer- oder Migrationsbehörden oder auch an grosse Verkehrsbetriebe oder, rechtsmedizinische Institute, die auch unter den Behördenbegriff fallen dürften (vgl. oben). Ebenso bestimmte Behörden des Bundes wie das BAZG oder Zoll- und Steuerbehörden des Bundes.

Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf die gemeinsame kantonale Datenbank erfolgen. Dafür braucht es unseres Erachtens keine Quittung. Die Protokollierung in den Logfiles des kantonalen IT-Systems genügt. Aus Sicht des Datenschutzes und der IT-Sicherheit ist die Mutation von Zugriffsrechten dem mehrmaligen Versand von Dokumenten über eine externe Plattform klar vorzuziehen.

Die Voraussetzungen von Art. 24 des Entwurfs sollten sich wiederum an Artikel 23 orientieren und nicht darüber hinausgehen. Es ist nicht ersichtlich, weshalb Artikel 24 strengere Anforderungen vorsieht, da Artikel 103c Absatz 2 StPO – anders als Art. 103b Absatz 2 StPO mit der Feststellung der Zeitpunkte der Übermittlung und dem Schutz der Akte vor Veränderung und unberechtigter Kenntnisnahme - überhaupt keine weiteren Anforderungen an die Dokumentation einer Übermittlung stellt.

10. Inkraftsetzung

Gemäss aktuellem Kenntnis- und Planungsstand ist die Inkraftsetzung des VEKJ auf Q2 2027 vorgesehen. Die SSK begrüsst eine möglichst zeitnahe Inkraftsetzung der Verordnungen zum BEKJ. Hier ist jedoch für die Staatsanwaltschaften Verbindlichkeit erforderlich. Die zahlreichen organisatorischen Anpassungen benötigen Planungssicherheit.

11. Aufhebung und Änderung anderer Erlasse

Durch die Aufhebung der Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren können IncaMail und PrivaSphere in Verfahren, die nach dem Inkrafttreten der Verordnung begonnen haben, nicht mehr genutzt werden.

Für Verwaltungsverfahren, welche nicht über die Plattform justitia.swiss abgewickelt werden können, sind geeignete Kanäle auszuwählen und bereit zu stellen.

Auch die Staatsanwaltschaften führen in begrenztem Umfang Verwaltungsverfahren (Akteneinsicht in abgeschlossene Verfahren, Ermächtigungsverfahren, TEVG-Verfahren, Personal-Geschäfte). Ziel sollte eine möglichst bürgerfreundliche Kommunikation über einen Kanal sein. Dies für Straf- und Verwaltungsverfahren. Gerade die Akteneinsicht zeigt deutlich auf, wieviel Verwirrung die aktuelle Regelung stiftet: Während dem Verfahren richtet sich die Einsicht nach Art. 101 StPO und damit erfolgt sie über die Plattform justitia.swiss in Anwendung von Art. 1 Abs. c BEKJ. Die Einsicht in abgeschlossene Verfahren wiederum richtet sich nach den kantonalen Datenschutzgesetzen im Rahmen eines nichtstrittigen Verwaltungsverfahrens und geht damit über andere Kanäle. Das Beschwerdeverfahren gegen eine allfällig verweigerte oder beschränkte Einsicht ist ein strittiges Verwaltungsverfahren und wäre somit wieder über die Plattform justitia.swiss abzuwickeln. Solche Szenarien sind und können verhindert werden, wenn die Nutzung der Plattform auch für nicht strittige Verwaltungsverfahren zugelassen würde.

Für die Berücksichtigung unserer Anliegen danken wir bestens.

Freundliche Grüsse



Christoph Ill, Präsident SSK
Erster Staatsanwalt des Kantons St. Gallen

Kopie:
- Mitglieder SSK
- Generalsekretariat KKJPD
- Generalsekretariat KKPKS

Von:	Verband
An:	Perler Cornelia BJ
Betreff:	AW: Verordnung zum neuen BEKJ-Gesetz / Ordonnance sur la nouvelle loi LPCJ / Ordinanza sulla nuova legge LCEG
Datum:	Montag, 16. März 2026 15:03:14
Anlagen:	image001.png

Achtung: Diese E-Mail stammt von einer externen Quelle. Bitte prüfen Sie den Inhalt mit besonderer Sorgfalt.
Attention: cet e-mail provient d'une source externe. Veuillez en vérifier le contenu avec la plus grande vigilance.
Attenzione: questa e-mail proviene da una fonte esterna. La preghiamo di verificarne attentamente il contenuto.

Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit zur eingangs erwähnten Vernehmlassung Stellung nehmen zu können.

Da diese Vorlage aufgrund der Dossieraufteilung zwischen economiesuisse und dem Schweizerischen Arbeitgeberverband von ersterem behandelt wird, verzichtet der Schweizerische Arbeitgeberverband auf eine Stellungnahme zu dieser Vernehmlassung.

Wir danken Ihnen bestens für Ihre Kenntnisnahme.

Mit freundlichen Grüssen

Isabelle Pantò

Isabelle Pantò-Herrnberger
Assistentin

Schweizerischer
Arbeitgeberverband
Hegibachstrasse 47
Postfach, 8032 Zürich

D: +41 44 421 17 42

arbeitgeber.ch | LinkedIn | X

Die Arbeitgeber
Les Employeurs
Gli Imprenditori

Schweizerischer Blindenbund
Selbsthilfe blinder und sehbehinderter Menschen

Zürich, 22.06.2026

GEMEINSAM NACH VORNE SEHEN.

Geschäftsstelle
Friedackerstrasse 8
8050 Zürich
Tel. 044 317 90 00
info@blind.ch; www.blind.ch

Vorsteher des Eidgenössischen Justiz- und Polizeidepartements EJPD

Per E-Mail an:
cornelia.perler@bj.admin.ch

Dateiformat: gleichlautend als PDF und Word

Vernehmlassungsantwort zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Stellungnahme des Schweizerischen Blindenbundes

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren

Der Schweizerische Blindenbund (SBb) nimmt die Gelegenheit wahr, zum rubrizierten Thema Stellung zu nehmen.

Der SBb begrüsst das Ziel der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ), die rechtlichen Grundlagen für durchgängig digitale Justiz- und Verwaltungsverfahren auf Verordnungsstufe zu konkretisieren und damit die Umsetzung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) zu ermöglichen.

Allgemeines

Im Hinblick auf die Aspekte der Digitalisierung dieser Vorlage weisen wir darauf hin, dass die Barrierefreiheit (Accessibility und Usability) gewährleistet sein muss, um die Zugänglichkeit für alle Personen (einschliesslich Menschen mit Behinderungen) sicherzustellen. Unter Einbezug entsprechender Fachstellen und -personen lassen sich personelle und finanzielle Ressourcen minimieren und spätere Zusatzkosten vermeiden. Mit einer Verankerung des Barrierefreiheitsaspekts in der Vernehmlassungsvorlage werden die diesbezüglich geltenden, rechtlichen Bestimmungen vollzogen

(Behindertengleichstellungsgesetz [BehiG, SR 151.3], Konvention über die Rechte von Menschen mit Behinderungen [BRK, SR 0.109]).

Fehlende Barrierefreiheitsanforderungen in Art. 2 VEKJ

Die VEKJ regelt in Art. 2 Abs. 1 die Betriebsvoraussetzungen für Plattformen nach dem BEKJ. Die Bestimmung nennt Anforderungen an Datenschutz, Verschlüsselung, Dokumentengrösse und Löschbarkeit. Eine ausdrückliche Anforderung zur Barrierefreiheit der Plattformen ist hingegen nicht vorgesehen.

Der Zugang zu Justiz- und Verwaltungsverfahren ist ein grundlegendes Recht. Für Menschen mit Sehbehinderung, Hörsehbehinderung, Blindheit oder Taubblindheit ist dieser Zugang nur dann gewährleistet, wenn die eingesetzten Plattformen vollständig mit assistiven Technologien nutzbar sind. Plattformen, die diese Anforderung nicht erfüllen, schliessen betroffene Personen faktisch vom elektronischen Rechtsverkehr aus, was dem BehiG sowie den Vorgaben der BRK widerspräche.

Zu berücksichtigen ist zudem, dass die bestehenden Barrierefreiheitsvorgaben des Bundes diesen Bereich nicht abdecken: Die Weisung W013 des Bereichs Digitale Transformation und IKT-Lenkung (DTI), welche die Barrierefreiheit digitaler Angebote der Bundesverwaltung regelt und auf den technischen Standard eCH-0059 verweist, gilt ausdrücklich nur für öffentlich zugängliche Informationen wie Websites, mobile Anwendungen und öffentliche Dokumente. Die Plattformen nach BEKJ sind demgegenüber geschlossene Verfahrensplattformen mit beschränktem Zugang und fallen damit nicht in den Anwendungsbereich der W013.

Eine Verankerung der Barrierefreiheitspflicht auf Verordnungsstufe ist daher angezeigt. Anwältinnen und Anwälte, Behördenmitarbeitende und andere dem Obligatorium unterstehende Personen mit Sehbehinderung, Blindheit oder Taubblindheit sind auf die Barrierefreiheit dieser Plattformen in gleichem Masse angewiesen wie auf jene öffentlicher Angebote. Das Obligatorium zur elektronischen Kommunikation nach BEKJ macht die Nutzung der Plattformen zur Rechtspflicht - eine Pflicht, die ohne barrierefreie Umsetzung für Menschen mit den genannten Beeinträchtigungen faktisch nicht erfüllbar ist.

Art. 2 Abs. 2 VEKJ bietet mit der Delegationsnorm an das EJPD eine geeignete Grundlage, Barrierefreiheitsanforderungen in der Departementsverordnung technisch zu präzisieren. Sinnvollerweise setzt dies eine entsprechende Verankerung als Betriebsvoraussetzung in Art. 2 Abs. 1 VEKJ voraus.

Anträge

- Art. 2 Abs. 1 VEKJ ist um folgenden Buchstaben e zu ergänzen:
«e. Die Plattform ist barrierefrei zugänglich und kann vollständig mit assistiven Technologien genutzt werden.»

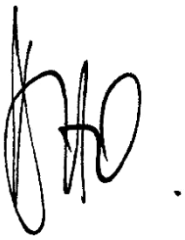
- Zudem ist das EJPD im Rahmen von Art. 2 Abs. 2 VEKJ zu verpflichten, in der Departementsverordnung die Barrierefreiheitsanforderungen an die Plattformen verbindlich zu konkretisieren. Als technischer Referenzstandard sind dabei die Web Content Accessibility Guidelines (WCAG) auf Konformitätsstufe AA heranzuziehen. Die Anforderungen gelten unabhängig davon, ob eine Plattform öffentlich oder nur einem beschränkten Nutzendenkreis zugänglich ist.

Der Schweizerische Blindenbund dankt Ihnen für die Prüfung und Berücksichtigung seiner Anliegen im Interesse blinder und sehbehinderter Menschen.

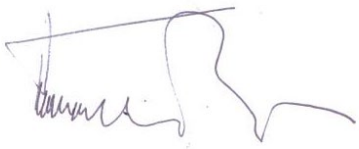
Freundliche Grüsse

Schweizerischer Blindenbund

Daniel Hörschläger
Geschäftsführer



Roland Gossweiler
Delegierter des Vorstandes für Sozialpolitik und Interessenvertretung



SGB | USS
www.sgb.ch | www.uss.ch
Schweizerischer Gewerkschaftsbund
Union syndicale suisse
Unione sindacale svizzera

Eidgenössisches Justiz- und Polizeidepartement
(EJPD)
Herr Bundesrat Jans

Bundeshaus West
CH-3003 Bern

Bern, 02. Juli 2026

per Mail an:
cornelia.perler@bj.admin.ch

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ): Stellungnahme des Schweizerisches Gewerkschaftsbundes (SGB)

Sehr geehrter Herr Bundesrat Jans

Besten Dank für die Einladung zur oben erwähnten Vernehmlassung.

Der Schweizerische Gewerkschaftsbund (SGB) unterstützt die Digitalisierung des Rechtsverkehrs. Der elektronische Rechtsverkehr ist Teil einer modernen staatlichen Grundversorgung. Voraussetzung dafür ist jedoch, dass Sicherheit, Datenschutz, diskriminierungsfreier Zugang und die öffentliche Verantwortung jederzeit gewährleistet bleiben. Der elektronische Rechtsverkehr muss Teil einer gerechten Digitalisierung sein. Er soll den Zugang zur Justiz vereinfachen, ohne die prozessualen Rechte der Parteien faktisch oder rechtlich zu beeinträchtigen. Dabei ist insbesondere auf die folgenden Punkte hinzuweisen.

Allgemeine Bemerkungen und Zeitpunkt der Inkraftsetzung

Aus gewerkschaftlicher Sicht dient eine digitale, medienbruchfreie Kommunikation zwischen Parteien und Behörden der Effizienz des Justiz- und Verwaltungsverfahrens und vereinfacht dessen Zugänglichkeit.

Der SGB begrüsst, dass für den Betrieb dieser staatlichen Aufgabe eine öffentlich-rechtliche Körperschaft und nicht eine private Entität beauftragt wird. Dass der Bundesrat in Art. 2 VE-VEKJ die gleichen Anforderungen für die kantonalen Plattformen setzt und in Art. 3 VE-VEKJ ein Bewilligungsverfahren vorsieht, schafft einen staatlich festgesetzten Sicherheitsstandard.

Die Verpflichtung, Verfahren über eine Plattform abzuwickeln, kann insbesondere für kleinere und mittlere Anwaltskanzleien mit Umstellungsaufwand verbunden sein. Der SGB befürwortet deshalb einen späteren Zeitpunkt der Inkraftsetzung, damit den Betroffenen genügend Zeit für die Vorbereitung bleibt.

Einheitliches Schutzniveau

Die Informationen, die im elektronischen Rechtsverkehr ausgetauscht werden, sind hoch sensibel. Durch deren Missbrauch und durch die Störung von den Informationssystemen können die Rechte von den beteiligten Personen schwerwiegend verletzt werden, weshalb die Ausgestaltung des notwendigen Schutzes essenziell ist. Dieses Sicherheitsniveau muss schweizweit einheitlich ausgestaltet und gewährleistet werden. Deswegen begrüsst der SGB insbesondere die in Art. 13 VE-VEKJ vorgesehene Anwendung auf die von den Kantonen zur Verfügung gestellten Plattformen des Informationssicherheitsgesetzes[1] und von Art. 8 des Datenschutzgesetzes.[2] Dadurch wird ein einheitliches Schutzniveau sichergestellt und Rechtsunsicherheit infolge einer gesetzlichen Fragmentierung vermieden. Ob bei der Benutzung der Plattform tatsächlich die datenschutzrechtlichen Vorschriften eingehalten werden und die ausreichende Datensicherheit angeboten wird, wird durch die Kontrollinstrumente des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) überprüft (Art. 27 Abs. 6 BEKJ).[3] Um diese Aufgaben gewährleisten zu können, muss er aber über ausreichende personelle und fachliche Ressourcen verfügen.

Der SGB teilt die *ratio legis* von Art. 12 VE-VEKJ, wonach die sechsmonatige Aufbewahrungsfrist dem Datenschutz und der Datensicherheit dienen sollte. Dennoch darf die sechsmonatige Aufbewahrungsfrist das Recht auf Zugang zu persönlichen Dokumenten nicht unverhältnismässig einschränken. Die Plattform sollte sicherstellen, dass die Benutzerinnen und Benutzer mehrmals über die zukünftige Vernichtung und deren Folgen informiert sind.

Universelles Authentifizierungsmittel

Der SGB begrüsst das in Art. 8 VE-VEKJ ausgewählte System «AGOV» für die Authentifizierung der Benutzerinnen und Benutzer der Plattformen. Dieser Authentifizierungsdienst ist zu befürworten, weil ein AGOV-Login von jeder Person mit einem gültigen Reisepass oder einer gültigen Identitätskarte erhalten werden kann und nicht, im Unterschied zur e-ID, der Schweizer Ausweis bzw. das Vorliegen einer Aufenthaltsbewilligung oder deren Antrag als Voraussetzung vorsieht. Letztlich sind Beschränkungen auf bestimmte Aufenthaltsbewilligungen nicht vorgesehen.[4] Gleichzeitig kann eine Person, die über eine schweizerische e-ID verfügt, ein AGOV-Login ohne weiteren Nachweis einrichten. AGOV trägt damit zu einer diskriminierungsfreien, sicheren und niederschwelligen digitalen Kommunikation im Justizverfahren bei.

Gebühr

Der SGB begrüsst die in Art. 15 und Art. 16 VE-VEKJ konkretisierte Pauschalerhebung von Gebühren durch den Bund und die Kantone statt einer individuellen Erhebung. Die Justiz stellt eine staatliche Aufgabe dar. Die Finanzierung einer für die Kommunikation der Behörden obligatorischen Plattform muss durch den Staat erfolgen. Die Kontrollen durch das EJPD gemäss Art. 15 Abs. 3 und Art. 21 VE-VEKJ sind in Zukunft sorgfältig durchzuführen, damit sichergestellt ist, dass die Körperschaft nicht gewinnorientiert betrieben wird.

Besten Dank für die Berücksichtigung unserer Stellungnahme.

---

[1] SR 128
[2] SR 235.1
[3] SR 172.023
[4] Vgl. Art. 14 E-ID-Gesetz sowie E-ID-Gesetz, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, S. 9.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND

Pierre-Yves Maillard
Präsident

Gabriela Medici
Co-Sekretariatsleiterin

SZBLIND
Schweizerischer Zentralverein
für das Blindenwesen

Vorsteher des Eidgenössischen Justiz- und
Polizeidepartements
EJPD

Per Mail an:
cornelia.perler@bj.admin.ch

Schweizerischer Zentralverein
für das Blindenwesen SZBLIND
Schützengasse 4
9001 St. Gallen

www.szblind.ch
jonas.pauchard@szblind.ch

St. Gallen, 28. Mai 2026

Vernehmlassungsantwort zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren

Der Schweizerische Zentralverein für das Blindenwesen SZBLIND bedankt sich für die Vorlage und die Möglichkeit zur Stellungnahme.

Der SZBLIND begrüsst das Ziel der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ), die rechtlichen Grundlagen für durchgängig digitale Justiz- und Verwaltungsverfahren auf Verordnungsstufe zu konkretisieren und damit die Umsetzung des Bundesgesetzes über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ) zu ermöglichen.

Allgemeines

Im Hinblick auf die Aspekte der Digitalisierung dieser Vorlage weisen wir darauf hin, dass die Barrierefreiheit (Accessibility und Usability) gewährleistet sein muss, um die Zugänglichkeit für alle Personen (einschliesslich Menschen mit Behinderungen) sicherzustellen. Unter Einbezug entsprechender Fachstellen und -personen lassen sich personelle und finanzielle Ressourcen minimieren und spätere Zusatzkosten vermeiden. Mit einer Verankerung des Barrierefreiheitsaspekts in der Vernehmlassungsvorlage werden die diesbezüglich geltenden, rechtlichen Bestimmungen vollzogen (Behindertengleichstellungsgesetz [BehiG, SR 151.3], Konvention über die Rechte von Menschen mit Behinderungen [BRK, SR 0.109]).

Fehlende Barrierefreiheitsanforderung in Art. 2 VEKJ

Die VEKJ regelt in Art. 2 Abs. 1 die Betriebsvoraussetzungen für Plattformen nach dem BEKJ. Die Bestimmung nennt Anforderungen an Datenschutz, Verschlüsselung, Dokumentengrösse und Löschbarkeit. Eine ausdrückliche Anforderung zur Barrierefreiheit der Plattformen ist hingegen nicht vorgesehen.

Der Zugang zu Justiz- und Verwaltungsverfahren ist ein grundlegendes Recht. Für Menschen mit Sehbehinderung, Hörsehbehinderung, Blindheit oder Taubblindheit ist dieser Zugang nur dann gewährleistet, wenn die eingesetzten Plattformen vollständig mit

assistiven Technologien nutzbar sind. Plattformen, die diese Anforderung nicht erfüllen, schliessen betroffene Personen faktisch vom elektronischen Rechtsverkehr aus, was dem BehiG sowie den Vorgaben der BRK widerspräche.

Zu berücksichtigen ist zudem, dass die bestehenden Barrierefreiheitsvorgaben des Bundes diesen Bereich nicht abdecken: Die Weisung W013 des Bereichs Digitale Transformation und IKT-Lenkung (DTI), welche die Barrierefreiheit digitaler Angebote der Bundesverwaltung regelt und auf den technischen Standard eCH-0059 verweist, gilt ausdrücklich nur für öffentlich zugängliche Informationen wie Websites, mobile Anwendungen und öffentliche Dokumente. Die Plattformen nach BEKJ sind demgegenüber geschlossene Verfahrensplattformen mit beschränktem Zugang und fallen damit nicht in den Anwendungsbereich der W013.

Eine Verankerung der Barrierefreiheitspflicht auf Verordnungsstufe ist daher angezeigt. Anwältinnen und Anwälte, Behördenmitarbeitende und andere dem Obligatorium unterstehende Personen mit Sehbehinderung, Blindheit oder Taubblindheit sind auf die Barrierefreiheit dieser Plattformen in gleichem Masse angewiesen wie auf jene öffentlicher Angebote. Das Obligatorium zur elektronischen Kommunikation nach BEKJ macht die Nutzung der Plattformen zur Rechtspflicht - eine Pflicht, die ohne barrierefreie Umsetzung für Menschen mit den genannten Beeinträchtigungen faktisch nicht erfüllbar ist.

Art. 2 Abs. 2 VEKJ bietet mit der Delegationsnorm an das EJPD eine geeignete Grundlage, Barrierefreiheitsanforderungen in der Departementsverordnung technisch zu präzisieren. Sinnvollerweise setzt dies eine entsprechende Verankerung als Betriebsvoraussetzung in Art. 2 Abs. 1 VEKJ voraus.

Anträge

- Art. 2 Abs. 1 VEKJ ist um folgenden Buchstaben e zu ergänzen:
  «e. Die Plattform ist barrierefrei zugänglich und kann vollständig mit assistiven Technologien genutzt werden.»
- Zudem ist das EJPD im Rahmen von Art. 2 Abs. 2 VEKJ zu verpflichten, in der Departementsverordnung die Barrierefreiheitsanforderungen an die Plattformen verbindlich zu konkretisieren. Als technischer Referenzstandard sind dabei die Web Content Accessibility Guidelines (WCAG) auf Konformitätsstufe AA heranzuziehen. Die Anforderungen gelten unabhängig davon, ob eine Plattform öffentlich oder nur einem beschränkten Nutzendenkreis zugänglich ist.

Wir danken Ihnen für die Berücksichtigungen unserer Anträge.

Freundliche Grüsse

Pierre-Alain Uberti
Geschäftsleiter

Jonas Pauchard
Fachperson Interessenvertretung

Dr. iur. **Fabio E. R. Scotoni**
8610 Uster

E-Mail fabio@esse.ch
Tel. 044 970 1503

Per IncaMail an: cornelia.perler@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Beat Jans
Bundeshaus West
3003 Bern

2026-05-10

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Ich danke für die Gelegenheit, mich im Rahmen der Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) äussern zu können.

1 Allgemeine Bemerkungen

1.1 Inkraftsetzung

Eine Inkraftsetzung auf den 1. Januar 2027 erscheint sportlich.

Mit dem Inkrafttreten des BEKJ wird Art. 130 ZPO[1] ersetzt mit einem neuen Wortlaut. Die neue Bestimmung verweist vollumfänglich auf das BEKJ.

Gleichzeitig hebt die VE-VEKJ die VeÜ-ZSSV auf. Art. 12b HRegV[2], Art. 16b Abs. 1 FMedV[3] und Art. 39 Abs. 2 GBV[4] sowie mehrere Verordnungen im Betreibungswesen verweisen aber noch auf die VeÜ-ZSSV und teils auf die frühere Fassung von Art. 130 ZPO, werden aber von der vorliegenden Vorlage nicht geändert. Es besteht deshalb Bedarf, diese Verordnungen je anzupassen. Ich gehe davon aus, dass die entsprechenden Anpassungen Gegenstand gesonderter Vernehmlassungsverfahren bilden werden.

Allein nur schon aufgrund der erforderlichen Vernehmlassungsverfahren und sich allenfalls daraus ergebenden Anpassungen für die HRegV, FMedV und GBV sowie das Schuldbetreibungs- und Konkurswesen scheint es mir nicht zweckmässig, ein abschliessendes Inkrafttreten per 1. Januar 2027 ins Auge zu fassen. Ich kann jedoch nicht darüber mutmassen, wann ein Inkrafttreten opportun sein wird – dies ist abhängig von den diversen betroffenen Behörden.

1.2 Gebühren

Die Nutzung der zentralen Plattform ist nach Art. 32 Abs. 1 BEKJ für die Behörden gebührenpflichtig, nicht jedoch für die anderen Nutzerinnen und Nutzern. Dies führt zu einer Gebührenunterdeckung, mindestens für Verwaltungsbehörden. Beispielsweise sieht Art. 6 AllgGebV[5] vor, dass Auslagen als Teil der Gebühr gelten und gesondert berechnet werden. Das heisst konkret: Heute kann Post-Porto bei Anwendbarkeit der AllgGebV in Rechnung gestellt werden. Aber

1 Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (Zivilprozessordnung, ZPO; SR 272).
2 Handelsregisterverordnung vom 17. Oktober 2007 (HRegV; SR 221.411).
3 Fortpflanzungsmedizinverordnung vom 4. Dezember 2000 (FMedV; SR 810.112.2).
4 Grundbuchverordnung vom 23. September 2011 (GBV; SR 211.432.1).
5 Allgemeine Gebührenverordnung vom 8. September 2004 (AllgGebV; SR 172.041.1).

Art. 15 ff. VE-VEKJ sehen eine pauschale jährliche Gebühr vor. Nicht nur fällt also der Ersatz der Zustellgebühren weg, sondern es kommt eine nur schwierig vorhersehbare Rückstellung in den Finanzhausalt der Zahlungspflichtigen: ein Rückgang der Einnahmen gekoppelt mit einer Zunahme der Ausgaben.

Ich rege deshalb zwecks Entlastung der aktuell ohnehin allgemein angespannten Budgets dazu an, eine nutzungsorientierte Abrechnung vertieft zu prüfen, welche klar und rechtssicher unter Porto oder Auslagen subsumiert werden kann.

1.3 Open-Source-Software

Art. 2 EMBAG[6] sieht die Geltung des EMBAG nur die Geltung für die zentrale Bundesverwaltung und die dezentrale Bundesverwaltung vor. Für letzteres besteht eine Ausnahmemöglichkeit. Die Parlamentsdienste, die eidgenössischen Gerichte und die Bundesanwaltschaft können sich dem EMBAG ganz oder teilweise davon durch Vereinbarung mit dem Bundesrat unterstellen.

Gemäss Art. 3 BEKJ strebt der Bund zum Aufbau und zum Betrieb der zentralen Plattform gemeinsam mit den interessierten Kantonen die Gründung einer öffentlich-rechtlichen Körperschaft mit eigener Rechtspersönlichkeit an. Diese ist definitionsgemäss nicht Teil der Bundesverwaltung. Das heisst, dass die Pflicht zur Nutzung und Veröffentlichung von Open-Source in Art. 9 EMBAG für diese neue Plattform nach BEKJ und VE-VEKJ nicht greift, weil die Körperschaft nicht in den Geltungsbereich des EMBAG fällt.

Die Zielsetzung des EMBAG, wie diese Art. 1 EMBAG definiert, ist das Schaffen von Voraussetzungen für die Zusammenarbeit unter Behörden verschiedener Gemeinwesen und mit Dritten beim Einsatz elektronischer Mittel zur Unterstützung der Erfüllung von Behördenaufgaben sowie den Ausbau und die Weiterentwicklung des Einsatzes von elektronischen Mitteln zur Unterstützung der Erfüllung von Behördenaufgaben. Mit Blick auf die im BEKJ beabsichtigte Möglichkeit alternativer Plattformen ist es für die Interoperabilität wertvoll und zweckmässig, den Quellcode von justitia.swiss zu veröffentlichen. Nicht zuletzt fördert offener Quellcode Transparenz und steigert damit das Vertrauen in die Plattform mehr, als dies ein privater Source-Code-Audit oder öffentlicher Intrusionstest allein könnte; diese genannten Massnahmen würden aber durch eine Quellcodeveröffentlichung auch nicht per se obsolet werden.

Meines Erachtens wäre es deshalb wünschenswert, *die Anwendbarkeit von Art. 9 EMBAG (etwa in der Vereinbarung nach Art. 3 Abs. 2 BEKJ) sicherzustellen.*

2 Zu den einzelnen Bestimmungen

2.1 Art. 2 Anforderungen an die Plattform

Zur Verschlüsselung: In Art. 2 Abs. 1 lit. b VE-VEKJ muss eine Plattform verschlüsselte Übermittlung von Dokumenten unterstützen. Sie muss aber auch die Dokumente verschlüsselt *aufbewahren.* Es erschliesst sich dabei aber weder aus der Norm selbst noch aus dem Bericht, wer die Schlüssel für die Entschlüsselung halten soll. Wenn die Dokumente gegenüber der Plattform selbst auch verschlüsselt sein sollen – wer soll sie dann entschlüsseln können? Ist eine End-zu-End-Verschlüsselung zwischen Empfängerin oder Empfänger und Absenderin oder Absender beabsichtigt?

Zu den technischen Standards: Gemäss Art. 2 Abs. 1 lit. b VE-VEKJ müssen Dokumente auf der Plattform nach den technischen Standards der Bundesverwaltung verschlüsselt werden. Streng genommen bedeutet diese Formulierung, dass alle anderen technischen Standards der Bundesverwaltung *e contrario* nicht erfüllt werden müssten. Sinnvollerweise würde dies klargestellt werden.

An anderer Stelle, nämlich in Art. 5 Abs. 1 lit. d Ziff. 1, Art. 7 Abs. 1 und Art. 24 Abs. 2 VE-VEKJ werden Hashwerte erwähnt. Der technische Standard, nach welchem diese Hashwerte zu berechnen sind, ist aber weder auf Verordnungsstufe spezifiziert noch durch eine Verweisung auf technische Standards der Bundesverwaltung gedeckt. Verschlüsselung stellt Vertraulichkeit sicher;

6 Bundesgesetz vom 17. März 2023 über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG; SR 172.019).

Hashwerte stellen Integrität sicher. Diese zwei Begriffe sind nicht fungibel. Nach meinem Dafürhalten wäre deshalb:

- Art. 2 Abs. 1 lit. b VE-VEKJ so zu ändern, dass er neu lautet «Die technische Verarbeitung der Dokumente auf der Plattform erfolgt nach Massgabe der technischen kryptografischen Standards der Bundesverwaltung.»; oder
- für die Hashwerte eine weitere Litera in Abs. 1 aufzunehmen, etwa: «b^{bis}. Die nach dieser Verordnung erforderlichen Hashwerte werden nach dem Standard […] der Bundesverwaltung berechnet.».

Der Nachvollziehbarkeit halber wäre es sodann begrüssenswert, wenn wenigstens die Erläuterungen zur Verordnung nach Art. 26 lit. a PublV[7] darauf hinweisen würden, *wo diese Standards eingesehen werden können.*

2.2 Art. 3 Bewilligungsverfahren

Zu Abs. 4: Was passiert im Moment des Bewilligungsentzugs mit Unterlagen, die sich in jenem Zeitpunkt auf der Plattform befinden? Was passiert, wenn Nutzende im Nichtwissen um den Bewilligungsentzug auf einer unbewilligten Plattform einreichen? Eine praxistaugliche Lösung für alle Fälle wird sich nicht in der Verordnung festlegen lassen. Wohl aber sollte die Verordnung *dem EJPD die nötigen Befugnisse einräumen, die Konsequenzen des Bewilligungsentzugs für laufende und abgeschlossene Verfahren in der Verfügung über den Bewilligungsentzug zu regeln.*

2.3 Art. 4 Format der Dokumente

Zu Abs. 1: Gemäss Angaben der Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen (KOST) sind nicht alle Versionen von PDF/A für die Archivierung geeignet. Man liest etwa: «PDF/A-3 ist als Format für die Langzeitarchivierung nicht geeignet. Archive sollten darauf hinwirken, dass Dokumente in der Verwaltung im Standard PDF/A-2u gespeichert werden.»[8] Eine voraussetzungslose Einschränkung auf die gemeinhin archivtauglichen Format PDF/A-1 oder PDF/A-2 wäre jedoch mit unverhältnismässigem Aufwand verbunden. Denn das verbreitete Produkt Microsoft Word kann in seiner aktuellen Version in Microsoft 365 nur PDF/A-3 erstellen. Andere Versionen des PDF/A-Standards müssen – vor Anbringen einer allfälligen elektronischen Signatur/Siegel und/oder einem Zeitstempel – zuerst konvertiert werden. Ich schlage deshalb folgende Regelung vor:

> «[1] Die verfahrensleitenden und die verfahrensbeteiligten Behörden erstellen ihre Dokumente zur Übermittlung an die Plattformen im Format PDF/A-1 oder PDF/A-2. Sie können auch spätere Versionen von PDF/A nutzen, sofern diese Dokumente keine Eigenschaften aufweisen, welche nicht auch mit PDF/A-2 vereinbar sind.
>
> [1bis] Die übrigen Verfahrensbeteiligten übermitteln ihre Dokumente im Format PDF oder PDF/A.»

Daneben existiert ein Standard für *barrierefreie PDF-Dokumente,* PDF/UA (ISO 32000-1). Dieser schliesst sich nicht mit PDF/A gegenseitig aus.[9] Mit Blick auf Art. 14 Abs. 2 BehiG[10] wäre wohl eine Verankerung der technischen Barrierefreiheit durch PDF/UA mindestens der von den verfahrensleitenden Behörden zweckmässig.

Zu Abs. 3: Es fehlen Angaben, welche konkreten Standards zu erfüllen sind, namentlich Normherausgeberin, Nummer und ggf. Ausgabe (bspw. für einen ISO-Standard: «ISO 19005-1:2005»).

---

7 Verordnung vom 7. Oktober 2015 über die Sammlungen des Bundesrechts und das Bundesblatt (Publikationsverordnung, PublV; SR 170.512.1).

8 Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen (KOST), PDF/A-3: Allgemeine Informationen, https://kost-ceco.ch/cms/pdf-a-3.html (abgerufen: 14. März 2026).

9 Uwe Dombeck/Francis Zinke/Birgit Peböck/Josephine Schwebler, Hinweise zu PDF-Dokumenten, in: Überwachungsstelle des Bundes für Barrierefreiheit von Informationstechnik (Hrsg.), Barrierefreie Dokumente in Lernkontexten, https://handreichungen.bfit-bund.de/bf-dokumente-lernkontext/formate/pdf/pdf-dokument.html (abgerufen: 10. Mai 2026).

10 Bundesgesetz vom 13. Dezember 2002 über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (Behindertengleichstellungsgesetz, BehiG; SR 151.3).

Zu Abs. 3 lit. d im Speziellen: Die angegebenen Videoformate sind blosse *Containerformate.* Die eigentlichen zu unterstützenden Audio-/Videoformate (Codecs) sind damit noch nicht ausreichend spezifiziert. Es müssten auch noch die zu unterstützenden Codecs angegeben werden, welche innerhalb dieser Container erlaubt sind.

2.4 Art. 5 Quittung

Der Bericht führt auf S. 17 aus: «Es ist nicht notwendig, den Namen der Plattform auf der Quittung aufzuführen, da dies aus dem von der Plattform angebrachten Siegel hervorgeht.»

Im Rahmen der internationalen Rechts-/Amtshilfe kann es jedoch sein, dass eine Quittung durch eine ausländische Behörde auf Papier ausgedruckt wird. Um für diesen Fall eine gewisse Beständigkeit der Information sicherzustellen, rege ich dazu an, dass die Bezeichnung der Plattform auf der Quittung erscheinen sollte, auch wenn sie an sich redundant ist.

2.5 Art. 9 Profile

Mit Blick auf die aktuelle Ausgestaltung der Plattform justitia.swiss bedarf dieser Artikel einer grundsätzlichen Klärung. Auf justitia.swiss bezeichnen Organisationsprofile auch Behörden, solange diese keine verfahrensleitenden Behörden sind. Diese Terminologie ist schwer verständlich. Ich rege deshalb generell dazu an, drei Kategorien von Profilen zu verwenden: private Organisationsprofile, behördliche Organisationsprofile und Profile verfahrensleitender Behörden.

Zu Abs. 2: Die Bezeichnung des Siegels genügt nicht, um die betreffende Behörde zu identifizieren. Es ist nämlich ohne Weiteres möglich, dass zwei Behörden gleich heissen. Beispielsweise können zwei Gemeinden X und Y beide je eine Verwaltungseinheit mit der Bezeichnung «Hochbauamt» haben, auf welche das Siegel ausgestellt wird. Das Zertifikat für das Anbringen eines Siegels wird auf eine UID-Einheit ausgestellt (Art. 2 lit. d ZertES[11]). Aber weder UIDG[12] noch UIDV[13] verlangen, dass bei einer Verwaltungseinheit präzisierende Angaben gemacht werden müssen. Somit ist eine Kollision der Common-Name-Attribute im Zertifikat aufgrund der UID-Register-Daten denkbar (vgl. auch Art. 6 VZertES). Wenn nicht der öffentliche Schlüssel hinterlegt werden soll, könnte auch die UID hinterlegt werden: Das Attribut organizationIdentifier (OID 2.5.4.97) im Zertifikat für ein Siegel enthält diese Information und identifiziert eine Behörde präziser.

Zu Abs. 3: Name und Postadresse genügen nicht, um eine Organisation zu identifizieren. Beispielsweise im Rahmen von Streitigkeiten über die Gründung eines Vereins kann es gut vorkommen, dass eventuell zwei potenzielle Vereine mit demselben Domizil unterschieden werden müssen. Es wäre meines Erachtens zielführender, die Plattform(en) zur UID-Stelle zu berufen, damit alle Organisationen eine Unternehmens-Identifikationsnummer (UID) angeben müssen. Ohne diese Angabe würden sie subsidiär von einer Plattform eine solche zugeteilt bekommen. Das UID-Register kann insbesondere auch einfache Gesellschaften, nicht im Handelsregister eingetragene Vereine und ausländische Rechtsformen erfassen, weshalb sich die Verwendung der UID anbietet.

2.6 Art. 11 Bestätigung und Entzug der Berechtigungen

Im Vorentwurf fehlt eine Regelung, wie mit einer (elektronischen und/oder schriftlichen) Unzustellbarkeit der Anfrage nach Art. 11 VE-VEKJ umzugehen ist.

Ich rege dazu an, ein schlankes Löschungsverfahren analog Art. 934*a* OR i.V.m. Art. 152 ff. HRegV in die Verordnung aufzunehmen.

Hintergrund und Grössenordnung: Im Schweizerischen Handelsamtsblatt finden sich unter dem Stichwort «Organisationsmangel» in der Rubrik «Bekanntmachungen nach

---

11 Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03).

12 Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG; SR 431.03).

13 Verordnung vom 26. Januar 2011 über die Unternehmens-Identifikationsnummer (UIDV; SR 431.031).

Handelsregisterverordnung» im Zeitraum vom 1. Januar 2025 bis und mit dem 31. Dezember 2025 insgesamt 2005 Meldungen (wobei eine Meldung mehr als eine Rechtseinheit betreffen kann). Das heisst konkret: über 2000 Rechtseinheiten waren mindestens vorübergehend postalisch nicht erreichbar. Im Jahr 2024 wurden gemäss der Statistik «Konkursverfahren und Betreibungshandlungen» des Bundesamts für Statistik aufgrund von Organisationsmängeln 2835 Rechtseinheiten aufgelöst.[14]

2.7 Art. 14 Virenprüfung

Zu Abs. 4: Die Durchführung einer Prüfung auf Schadsoftware entspricht gängiger Praxis und ist an sich zu begrüssen. Meiner Einschätzung nach verleitet die Markierung von nicht geprüften Dateien in Abs. 4 die Nutzenden indes zu einem falschen Gefühl von Sicherheit.

Die Prüfung von Schadsoftware ist nicht über alle Zweifel erhaben. Denkbar ist nämlich auch, dass eine neuartige Schadsoftware entwickelt wird, spezifisch um Zugriff auf die Rechner einer verfahrensleitenden Behörde zu erlangen. Da diese Software neuartig ist und gerade mit diesem Ziel entwickelt sowie hierfür getestet wurde, kann eine Prüfung auf Schadsoftware hin wirkungslos verpuffen. Die Schadsoftwareprüfung allein ist daher kein Garant für eine sichere Datei.

Meines Erachtens wäre es deshalb sinnvoller, Dateien nicht bloss binär als «geprüft und in Ordnung» und «Schadsoftware» zu kennzeichnen. Vielmehr sollten Resultat, Schadsoftwareprüfungsprogramm und Zeitpunkt der Prüfung auch bei einer durchgeführten Prüfung eingeblendet werden. Diese Anzeige sollte begleitet werden von einer ständigen Warnung, dass die erfolgreich bestandene Schadsoftwareprüfung als solche nicht bedeutet, dass die Datei zwingend sicher ist.

Zu Abs. 5: Die im Bericht erwähnten Angaben über die nicht angenommenen Dokumente auf der Quittung entbehren einer rechtlichen Grundlage in der Verordnung und sollten deshalb in den Verordnungstext überführt werden.

2.8 Art. 22 Digitalisierung von physischen Dokumenten

Siehe Bemerkungen zu Art. 4 oben.

2.9 Aufhebung und Änderung anderer Erlasse, Ziff. II (Verordnung vom 23. November 2016 über die elektronische Signatur)

Zu Art. 14a: Der verwendete Begriff «Validator» in Art. 14*a* VE-VZertES ist soweit ersichtlich weder im ZertES noch im VZertES definiert. In der Annahme, dass das Validatorsystem unter https://www.validator.admin.ch/ bzw. die technische API für den diskreten Validator damit gemeint ist: Art. 19 EÖBV[15] bezeichnet dieses als «Validatorsystem des Bundes». Es wäre der Rechtssicherheit und Nachvollziehbarkeit dienlich, wenn diese beiden Bestimmungen eine einheitliche Terminologie verwenden würden.

Zu Art. 14b: Mit Blick auf einen allfälligen Markteintritt einer alternativen Plattform: Es wäre wünschenswert, wenn das BAKOM ermächtigt und verpflichtet würde, die berücksichtigten internationalen Normen gebührenfrei zu veröffentlichen, soweit es auf diese verweist.[16]

3 Schlussbetrachtung

Die Digitalisierung der Justiz ist ein anspruchsvolles Unterfangen, das wirtschaftliche, technische und rechtliche Implikationen auf das gesamte Rechtsdurchsetzungssystem der Schweiz auf allen Stufen hat. Vor diesem Hintergrund ermuntere ich dazu, dieses Vorhaben mit den

---

14 Bundesamt für Statistik, Konkursverfahren und Betreibungshandlungen, https://www.bfs.admin.ch/asset/de/34907021 (abgerufen: 14. März 2026).

15 Verordnung vom 8. Dezember 2017 über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV; SR 211.435.1).

16 Der Kanton Zürich kennt eine solche Bestimmung in § 8 Abs. 2 des Publikationsgesetzes vom 30. November 2015 (PublG; LS 170.5). Vgl. zur allgemeinen Problematik privater Normen FELIX UHLMANN, «Die Normen können bei … bezogen werden» – Gedanken zur Publikation und Verbindlichkeit privater Normen, in: LeGes 2013/1, S. 89 ff.; vgl. weiter CHRISTIAN BOCK, Der Umgang des Staates mit «technischen» Normen, in: Felix Uhlmann (Hrsg.), Private Normen und staatliches Recht: 14. Jahrestagung des Zentrums für Rechtsetzungslehre, Zürich/St. Gallen 2015, S. 42 f. im Speziellen.

sämtlichen tangierten Stakeholdern vertieft abgestimmt weiterzutreiben, insbesondere mit Fachstellen für Gleichstellung, Cybersicherheit und Kryptografie sowie mit den betroffenen Gerichts- und Verwaltungsbehörden. Insbesondere sollten auch nötige technische Anpassungen weder zeitlich noch finanziell unterschätzt werden.

Mit freundlichen Grüssen

Fabio E. R. Scotoni
eingebend als Privatperson

STELLUNGNAHME DER STADT USTER ZUR VERORDNUNG ÜBER DIE ELEKTRONISCHE KOMMUNIKATION IN BUNDESRECHTLICHEN JUSTIZ- UND VERWALTUNGSVERFAHREN (VEKJ)

Sehr geehrte Damen und Herren

Die Stadt Uster begrüsst die grundsätzliche Zielsetzung der VEKJ. Eine sichere, verbindliche und medienbruchfreie elektronische Kommunikation in Justiz- und Verwaltungsverfahren ist ein wichtiger Schritt in der digitalen Transformation der öffentlichen Verwaltung.

Die Vorlage dient der Umsetzung des BEKJ und regelt unter anderem den Betrieb der Plattformen, Authentifizierung, Benutzerkonten, Dokumentformate, Quittungen, Siegel, Schnittstellen, Aufbewahrung sowie Gebühren. Für die vom BEKJ erfassten Justizverfahren bildet justitia.swiss die zentrale Plattform. Die VEKJ regelt jedoch darüber hinaus auch weitere Plattformen nach BEKJ sowie die Plattform für Verwaltungsverfahren des Bundes.

Aus Sicht der Stadt Uster ist entscheidend, dass die Umsetzung nicht nur rechtlich und technisch korrekt, sondern auch für Städte und Gemeinden praxistauglich ist. Die kommunale Ebene ist organisatorisch sehr unterschiedlich aufgestellt. Aufgaben können zentral, dezentral, interkommunal oder durch eigenständige Organe wahrgenommen werden. Entsprechend braucht es klare Vollzugshilfen, stabile Schnittstellen, realistische Einführungsfristen und transparente Kostenfolgen.

1. Klare Abgrenzung der betroffenen kommunalen Behörden und Prozesse

Für Städte und Gemeinden muss frühzeitig klar sein, welche kommunalen Behörden und Prozesse in welchen Konstellationen von der VEKJ beziehungsweise von justitia.swiss betroffen sind. Der erläuternde Bericht hält fest, dass bei Kantonen und Gemeinden insbesondere Gerichte, Staatsanwaltschaften und Polizeien ab Inkrafttreten über ein Konto auf der zentralen Plattform verfügen müssen. Die übrigen Behörden können ein Onboarding bei Bedarf vornehmen, wenn sie erstmals mit Gerichten, Staatsanwaltschaften, Polizeien oder Verwaltungseinheiten des Bundes kommunizieren müssen.

Für die kommunale Praxis braucht es dazu eine verständliche Übersetzung. Je nach Gemeinde können Stadt- und Gemeindepolizeien, Betreibungsämter, Rechtsdienste, Fachabteilungen, Kommissionen, eigenständige Behörden oder interkommunale Stellen betroffen sein. Es ist zu klären, welche Prozesse zwingend über justitia.swiss beziehungsweise eine Plattform nach VEKJ abzuwickeln sind, welche Prozesse weiterhin über andere zulässige elektronische Kanäle laufen können oder müssen und wie die Abgrenzung zu bestehenden kantonalen, kommunalen oder fachspezifischen Lösungen erfolgt.

Die Stadt Uster regt deshalb an, dass der Bund gemeinsam mit Kantonen, Städten und Gemeinden eine konkrete Vollzugshilfe für die kommunale Ebene erarbeitet. Diese sollte typische Nutzungsszenarien, Behördenprofile, Zuständigkeiten, Stellvertretungen, Berechtigungen, Siegel, Schnittstellen, Supportprozesse sowie Onboarding- und Offboarding-Prozesse abbilden.

2. Rollen, Berechtigungen, Support und Betrieb

AGOV als Standard für die Authentifizierung wird von der Stadt Uster begrüsst. Die VEKJ sieht AGOV für die vom Bund bereitgestellte Plattformen vor, zudem werden mehrere Profile pro Benutzerkonto ermöglicht, Behördenprofile mit Mindestangaben geführt und erteilte Berechtigungen müssen regelmässig bestätigen werden.

Für Städte und Gemeinden ist dies jedoch nicht nur eine Login-Frage. Entscheidend ist das Betriebsmodell dahinter: Wer darf für welche Behörde rechtsverbindlich abrufen oder zustellen? Wie werden Stellvertretungen, Funktionswechsel, Austritte, Ferienvertretungen und autonome Behörden

abgebildet? Wer ist für Benutzerpflege, Profilverwaltung, Berechtigungsprüfung, Support und Systempflege verantwortlich?

Aus Sicht der Stadt Uster braucht es für unterschiedliche Gemeindegrössen unterschiedliche Rollen-, Berechtigungs- und Betriebskonzepte als Mustervorlagen. Eine kleine Gemeinde benötigt ein anderes Modell als eine grössere Stadt mit mehreren Abteilungen, Stadtpolizei, Kommissionen und spezialisierten Fachstellen. Ergänzend sollten Schulung und gemeindespezifisches Coaching für die Einführung aufgebaut werden.

3. Integration in GEVER- und Fachsysteme sicherstellen

Die Vorlage verlangt, dass Behörden ihre Dokumente zur Übermittlung im Format PDF/A erstellen. Beilagen können in jedem Format übermittelt werden, wobei die verfahrensleitende Behörde bestimmte Standardformate bearbeiten können muss. Zudem müssen Quittungen, Siegel, Zeitstempel, Hashwerte und Berechtigungen korrekt verarbeitet werden.

Für Stadtverwaltungen bedeutet dies: Die elektronische Kommunikation muss in bestehende GEVER- und Fachsysteme integriert werden können. Viele GEVER-Systeme erzeugen bereits PDF/A-Dokumente und unterstützen Signatur- oder Siegelprozesse. Wenn Dokumente dagegen manuell exportiert, separat gesiegelt, auf eine Plattform hochgeladen und Quittungen anschliessend wieder manuell abgelegt werden müssen, entstehen neue Medienbrüche statt echter Digitalisierung.

Der erläuternde Bericht sieht ausdrücklich Schnittstellen vor, über die Fachanwendungen und Geschäftsverwaltungssoftware Dokumente automatisch übermitteln oder abrufen können. Die Schnittstellen der zentralen Plattform sowie der Plattform nach Art. 6a Abs. 2 VwVG sollen kostenlos benutzbar sein. Aus Sicht der Stadt Uster müssen diese Schnittstellen frühzeitig, vollständig dokumentiert, stabil, standardisiert und für die gängigen GEVER- und Fachsysteme nutzbar sein. Städte und Gemeinden sollten in die Erarbeitung einbezogen werden.

4. Aktenführung, Export und Aufbewahrung

Die VEKJ sieht vor, dass auf der Plattform gespeicherte Dokumente und Quittungen sechs Monate nach Entgegennahme beziehungsweise Erstellung automatisch vernichtet werden. Bei Dokumenten zur Akteneinsicht bestimmt die verfahrensleitende Behörde, wie lange diese abrufbar sind; danach werden sie ebenfalls vernichtet.

Damit ist klar: Die Plattform ersetzt keine rechtskonforme Aktenführung der Behörden. Städte und Gemeinden müssen sicherstellen können, dass Dokumente, Quittungen, Abrufinformationen u.Ä. rechtzeitig und vollständig in ihre GEVER-Systeme übernommen werden.

Dafür braucht es praxistaugliche Export- und Schnittstellenfunktionen. Der Export darf nicht nur als manueller Download einzelner Dokumente ausgestaltet sein. Notwendig sind strukturierte Metadaten, maschinenlesbare Quittungen und automatisierte Ablageprozesse. Andernfalls entstehen administrativer Mehraufwand und Risiken für unvollständige Akten.

5. Anschlussfähigkeit an Bürgerportale prüfen

Die Vorlage sieht auch Profile für natürliche Personen vor. Gleichzeitig hält der erläuternde Bericht fest, dass für Personen, die dem Obligatorium nicht unterstehen, der bisherige Ablauf in der Kommunikation mit der Justiz unverändert bleibt. Die Plattform soll aber auch für Personen und Unternehmen attraktiv sein, die dem Obligatorium nicht unterstehen.

Soweit natürliche Personen die Plattform freiwillig nutzen können oder künftig elektronische Zustellungen an sie erfolgen, sollte die Anschlussfähigkeit an bestehende oder künftige kommunale

Bürgerportale geprüft und ermöglicht werden. Städte investieren zunehmend in digitale Bürgerkonten, sichere Posteingänge und serviceorientierte Portale. Es sollte vermieden werden, dass für Einwohnerinnen und Einwohner zusätzliche isolierte digitale Postfächer entstehen, wenn eine sinnvolle Integration oder Weiterleitung möglich wäre.

6. Kostenfolgen transparent und fair regeln

Die Gebührenregelung sieht vor, dass die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform über Gebühren gedeckt werden. Der Bund trägt gemäss Entwurf 10 Prozent, die Kantone 90 Prozent; der Kantonsanteil wird nach ständiger Wohnbevölkerung verteilt.

Die Vorlage regelt jedoch nicht abschliessend, welche indirekten Kosten auf Städte und Gemeinden zukommen. Neben allfälligen Gebühren betrifft dies insbesondere Aufwände für Schnittstellen, Anpassungen an GEVER- und Fachsystemen, Siegel, Schulung, Benutzerverwaltung, Betriebssupport und organisatorische Umstellungen.

Die Stadt Uster regt deshalb an, dass der SSV gegenüber Bund und Kantonen transparente, planbare und faire Kostenfolgen verlangt. Es darf nicht zu einer ungeregelten Kostenverschiebung auf Städte und Gemeinden kommen, insbesondere wenn kommunale Behörden rechtlich oder faktisch auf die Nutzung der Plattformen angewiesen sind.

7. Realistische Einführungsplanung und Einbezug der kommunalen Ebene

Als frühestmöglicher Zeitpunkt für die abschliessende Inkraftsetzung von BEKJ und VEKJ wird der 1. Januar 2027 genannt. Die Inkraftsetzung löst die Übergangsfristen betreffend Obligatorium aus.

Aus Sicht der Stadt Uster ist dieser Zeitpunkt nur realistisch, wenn Plattformen, Schnittstellen, Betriebskonzepte, Onboarding-Vorgaben, Supportprozesse und Schulungsunterlagen frühzeitig produktionsreif vorliegen. Die kommunale Ebene sollte deshalb verbindlich in die weitere Konkretisierung einbezogen werden. Städte und Gemeinden sind nicht nur mittelbar betroffen, sondern müssen die Vorgaben in sehr unterschiedlichen Organisationsformen konkret umsetzen.

Zusammenfassende Haltung

Die Stadt Uster begrüsst die Zielsetzung der VEKJ. Entscheidend ist jedoch, dass die Umsetzung für Städte und Gemeinden praxistauglich, finanzierbar und anschlussfähig an bestehende Verwaltungsprozesse erfolgt.

Der Bund soll klarstellen, welche kommunalen Behörden und Prozesse in welchen Konstellationen betroffen sind und wie Städte und Gemeinden justitia.swiss beziehungsweise Plattformen nach VEKJ organisatorisch und technisch nutzen sollen. AGOV wird als Standard begrüsst, muss aber durch praxistaugliche Rollen-, Berechtigungs-, Support- und Betriebskonzepte ergänzt werden. Für unterschiedliche Gemeindegrössen sind Best-Practice-Vorlagen sowie Schulungs- und Coachingangebote bereitzustellen.

Für PDF/A, Siegel, Zeitstempel, Quittungen und Aktenführung sind Schnittstellen zu GEVER- und Fachsystemen zentral. Die automatische Vernichtung von Dokumenten auf der Plattform macht praxistaugliche Export- und Ablagefunktionen erforderlich. Soweit natürliche Personen die Plattform freiwillig nutzen können oder künftig elektronische Zustellungen an sie erfolgen, sollte die Anschlussfähigkeit an kommunale Bürgerportale geprüft werden. Schliesslich sind die Kostenfolgen für Städte und Gemeinden transparent, planbar und fair zu regeln.

Freundliche Grüsse

Stadt Uster

Lucas Nicolussi
CDO

Marc Epelbaum
Direktwahl 041 419 55 00
marc.epelbaum@suva.ch

Suva
Generalsekretariat
Postfach
6002 Luzern

Herr
Bundesrat Beat Jans
Eidgenössisches Justiz-
und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

22. Juni 2026

Vernehmlassung Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, im Rahmen der Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ) Stellung nehmen zu können.

Die Suva ist die grösste Trägerin der obligatorischen Unfallversicherung in der Schweiz sowie Durchführerin der Militärversicherung. Die Suva ist eine autonome öffentlich-rechtliche Anstalt (Art. 6 Abs. 1 UVG) und gilt deshalb im Sinne des Verwaltungsverfahrensgesetzes (VwVG) als Behörde (Art. 1 Abs. 2 lit. c VwVG). Die Suva führt im Anwendungsbereich des BEKJ schwergewichtig sozialversicherungsrechtliche Verfahren vor kantonalen Verwaltungsgerichten und dem Bundesgericht. Daneben fallen Prämien- und Unterstellungsverfahren sowie Konkursverfahren im Zusammenhang mit ausstehenden Prämien an. Ferner werden zivilrechtliche (insbesondere Haftpflicht-, Arbeits- und Mietrecht) sowie strafrechtliche Verfahren geführt.

Mit dem Bundesgesetz über die Plattformen für die elektronische Kommunikation (BEKJ) werden die rechtlichen Grundlagen geschaffen, um durchgängig digitale, medienbruchfreie Justizverfahren zu ermöglichen. Künftig soll der Rechtsverkehr in allen Straf-, Zivil- und Verwaltungsgerichtsverfahren des Bundes über eine digitale Kommunikationsplattform abgewickelt werden. Das dem sozialversicherungsrechtlichen Gerichtsverfahren vorgelagerte Administrativverfahren (sog. Einspracheverfahren) fällt hingegen nicht in den Anwendungsbereich des BEKJ, es richtet sich grundsätzlich nach dem Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG). Die Verlagerung dieser Verfahren auf den elektronischen Rechtsweg wird im Rahmen des Bundesgesetzes über die Informationssysteme in den Sozialversicherungen (BISS) sowie der darin vorgesehenen Anpassungen des ATSG geregelt werden.

Zusammenfassend kann demnach festgehalten werden, dass die Suva (wie auch die übrigen Unfallversicherungen aufgrund von Art. 1 lit. e VwVG) zwar eine Behörde im Sinne des VwVG ist, jedoch im Rahmen der im BEKJ geregelten Verfahren vor Justizbehörden keine hoheitliche Funktion wahrnimmt. Es stellt sich daher die Frage, ob die Definition als Behörde gemäss VwVG derjenigen gemäss BEKJ entspricht und der Suva die entsprechenden Verpflichtungen obliegen.

Im VE-VEKJ werden grundsätzlich drei verschiedene Verfahrensbeteiligte festgehalten: Behörden, natürliche Personen und Organisationen. Eine Definition dieser Begriffe ist weder dem BEKJ noch dem VE-VEKJ zu entnehmen. Für die Sozialversicherungen, welche Verwaltungsverfahren gemäss ATSG durchführen, stellt sich daher die Frage, ob sie unter den Begriff der Behörde oder Organisation zu subsumieren sind. Im Gegensatz zu Organisationen gelten für Behörden weitere Verpflichtungen, beispielsweise in Bezug auf die Siegelpflicht (Art. 22 Abs. 2 BEKJ i.V.m. Art. 9 Abs. 2 VE-VEKJ) oder das Format von Dokumenten (vgl. Art. 9 Abs. 2 VE-VEKJ).

Nach Ansicht der Suva ist es nicht sinnvoll, die Sozialversicherungen im Anwendungsbereich des BEKJ als Behörden zu definieren. Vielmehr geht sie davon aus, dass diese sinnvollerweise als Organisationen zu gelten haben, da die Sozialversicherungen in den entsprechenden Verfahren nicht als entscheidende bzw. verfügende Behörden, sondern als verfahrensbeteiligte Parteien auftreten und funktional deshalb nicht mit den Justizbehörden gleichzustellen sind.

Im Rahmen von Justitia 4.0 führt die Suva mit dem Sozialversicherungsgericht Zürich ein Pilotprojekt auf der Plattform justitia.swiss durch. Sowohl die Vertreterin von Justitia 4.0 als auch das Sozialversicherungsgericht vertreten dabei die Auffassung, dass die Suva auf der Plattform ein «Organisationsprofil» und nicht ein Profil für eine Behörde zu eröffnen hat. Diese Einordnung ist auch aus praktischer Sicht sachgerecht und wird von der Suva ausdrücklich begrüsst.

Zur Schaffung der erforderlichen Rechtssicherheit ist deshalb im Erlass zu präzisieren, unter welchen Begriff die Suva sowie die anderen Sozialversicherer zu subsumieren sind. Eine entsprechende Präzisierung sollte entweder im Verordnungsentwurf selbst oder zumindest in den Erläuterungen vorgenommen werden.

Wir bedanken uns für die Berücksichtigung unserer Stellungnahme im Voraus und stehen Ihnen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse



Marc Epelbaum
Generalsekretär

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Ausschliesslich per E-Mail an:
cornelia.perler@bj.admin.ch

Zürich, 29.05.2026

Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der festgesetzten Frist Stellung zur Teilrevision der «Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)» zu nehmen.

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft und betreibt das nationale Rücknahmesystem «Swico-Recycling» für Elektro- und Elektronikgeräte. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen rund 60'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von über 40 Milliarden Franken.

Zusammenfassung:

Swico begrüsst die Stossrichtung der vorliegenden Verordnung. Die Einführung einer einheitlichen Plattform für den elektronischen Rechtsverkehr stellt einen zentralen Schritt für die Digitalisierung der Justiz und Verwaltung dar und stärkt die Effizienz sowie Standortattraktivität der Schweiz.

Aus Sicht der Digitalwirtschaft ist jedoch entscheidend, dass die Umsetzung technologieneutral, innovationsfreundlich und wettbewerbsorientiert erfolgt. Insbesondere müssen Interoperabilität, offene Standards, klare Governance-Strukturen sowie verhältnismässige Anforderungen an Marktakteure sichergestellt werden.

Swico sieht jedoch in mehreren Bereichen Anpassungsbedarf, um die Ziele der Verordnung nachhaltig zu erreichen und gleichzeitig die Innovationskraft des digitalen Ökosystems in der Schweiz zu stärken. Zentral ist, dass in der Vorlage Unklarheiten zur Organisation und dem Betrieb, der Technologieneutralität, der Wettbewerbsneutralität, einem risikobasierter Sicherheitsansatz, der Finanzierung und der Authentifizierung adäquat klärt.

1 Allgemeine Würdigung

Die VEKJ ist ein wichtiger Baustein zur Umsetzung des digitalen Rechtsverkehrs und fügt sich in die strategische Transformation zu medienbruchfreien Verfahren ein. Die geplante zentrale Kommunikationsplattform kann zu erheblichen Effizienzgewinnen für Behörden, Gerichte und Verfahrensbeteiligte führen.

Swico unterstützt insbesondere die Schaffung einer einheitlichen digitalen Infrastruktur für Justiz- und Verwaltungsverfahren, die Standardisierung elektronischer Kommunikationsprozesse und die Förderung eines durchgängigen digitalen Prozesses ohne Medienbrüche ermöglicht. Gleichzeitig weist Swico darauf hin, dass die konkrete Ausgestaltung der Verordnung entscheidend für den Erfolg ist. Eine zu restriktive oder technisch spezifische Regulierung könnte Innovation hemmen und bestehende sowie neue Anbieter unverhältnismässig belasten.

2 Organisation und Betrieb der Plattform

Swico hinterfragt die vorgesehene Organisationsstruktur. Die Bündelung von Betrieb und Steuerung in einer öffentlich-rechtlichen Trägerschaft wie sie im Bundesgesetz und gemäss erläuterndem Bericht vorgesehen ist, birgt das Risiko unzureichender Marktöffnung und eingeschränkter Innovationsdynamik. Aus Sicht von Swico ist sicherzustellen, dass die Governance-Struktur transparent ausgestaltet wird, eine klare Trennung zwischen regulatorischen und operativen Funktionen erfolgt, und geeignete Mitwirkungsformate für private Akteure geschaffen werden. Ohne entsprechende Mechanismen besteht die Gefahr, dass die Plattform zu einer geschlossenen staatlichen Infrastruktur wird.

3 Technologieneutralität und offene Standards

Die Verordnung sollte konsequent technologieneutral formuliert werden. Vorgaben zu Formaten und Schnittstellen sind so auszugestalten, dass offene, international anschlussfähige Standards bevorzugt werden, keine implizite Bevorzugung einzelner Technologien oder Anbieter erfolgt und zukünftige technologische Entwicklungen integriert werden können. Swico empfiehlt, explizit auf offene Schnittstellen (APIs) und standardisierte Datenformate zu setzen, um Interoperabilität und Wettbewerb zu gewährleisten. Konkret geht es uns hier um die Art. 8 – 10 und Art. 22ff.

4 Marktzugang und Wettbewerb

Bestimmungen zum Zugang und zur Nutzung sind aus wettbewerbspolitischer Sicht von zentraler Bedeutung. Die Plattform darf nicht zu einer Verdrängung bestehender privater Lösungen führen oder den Wettbewerb verzerren. Die faktische Etablierung einer verpflichtenden Plattformlösung kann zu einer Verdrängung bestehender oder zukünftiger privater Angebote führen.

Wichtig ist ein diskriminierungsfreier Zugang für Anbieter von digitalen Dienstleistungen, Einbezug alternativer, gleichwertiger Lösungen privater Dienstleister, Vermeidung von Monopolstrukturen und klare Regeln für die Integration von Drittanbietern. Swico betont, dass ein funktionierendes Ökosystem aus privaten und öffentlichen Akteuren entscheidend für Innovation und Qualität ist. Die Verordnung macht keine konkreten Vorgaben zum Marktzugang und Wettbewerb, weshalb wir empfehlen, dies an einer entsprechenden Stelle vorzunehmen.

5 Datensicherheit und Datenschutz

Als zentrale Infrastruktur für sensible Verfahrensdaten muss die Plattform höchste Anforderungen an Sicherheit und Datenschutz erfüllen. Swico unterstützt dabei ein risikobasierter Sicherheitsansatz, Privacy-by-Design und Privacy-by-Default sowie transparente Regelungen zur Datenbearbeitung. Gleichzeitig ist darauf zu achten, dass Sicherheitsanforderungen verhältnismässig bleiben. Dem Prinzip des risikobasierten Sicherheitsansatzes ist zu folgen.

6 Identitätsmanagement und Authentifizierung

Die Regelungen zur Identifikation der Nutzerinnen und Nutzer sind zentral für die Funktionsfähigkeit der Plattform. Swico empfiehlt die Nutzung interoperabler und möglichst bestehender Identitätslösungen und die Vermeidung proprietärer Insellösungen. Die Anschlussfähigkeit an die e-ID begrüssen wir ausdrücklich.

7 Kosten- und Finanzierungsmodell

Die Finanzierung der Plattform muss transparent, fair und wirtschaftlich tragfähig ausgestaltet sein. Swico fordert die Vermeidung von unverhältnismässigen Kostenbelastungen für private Akteure und Anreize für effizienten Betrieb und Innovation.

8 Skalierbarkeit und Weiterentwicklung

Die Plattform ist als langfristige Infrastruktur zu verstehen. Entsprechend wichtig sind eine modulare Architektur, eine kontinuierliche Weiterentwicklung und die Offenheit für neue Anwendungsfälle und Technologien. Swico empfiehlt, die Verordnung so auszugestalten, dass iterative Verbesserungen möglich bleiben.

9 Schlussbemerkung

Swico unterstützt die Zielsetzung der VEKJ, den elektronischen Rechtsverkehr in der Schweiz entscheidend voranzubringen. Damit die Plattform ihr volles Potenzial entfalten kann, ist jedoch eine konsequent innovationsfreundliche, wettbewerbsorientierte und technologieneutrale Ausgestaltung der VEKJ erforderlich.

Swico steht bereit, den weiteren Prozess aktiv zu begleiten und die Perspektive der Digitalwirtschaft einzubringen.

Freundliche Grüsse
Swico



Dr. Jon Fanzun
CEO



Annika Bos
Public Affairs Manager

KANTON GLARUS
VERWALTUNGSKOMMISSION DER GERICHTE
GERICHTSHAUS, 8750 GLARUS, TELEFON 055 646 53 40

8750 Glarus, 8. Juni 2026

cornelia.perler@bj.admin.ch

Vernehmlassung zur Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ)

Sehr geehrte Damen und Herren

Im Namen der Verwaltungskommission der Gerichte des Kantons Glarus danke ich Ihnen für die Gelegenheit zur Vernehmlassung zum Entwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (VEKJ).

Wir haben zum Entwurf folgende Anmerkungen:

Ingress

Der Entwurf verzichtet darauf, im Ingress alle Delegationsnormen aufzuführen, auf welche sich die VEKJ stützt. Der Klarheit und Vollständigkeit halber wäre es jedoch vorzuziehen, wenn im Ingress sämtliche Delegationsnormen erwähnt würden.

Art. 2: Anforderungen an die Plattformen

Art. 2 Abs. 1 Bst. c sieht vor, dass die Plattform bis zu zwei Gigabyte grosse Dokumente entgegennehmen und übermitteln kann. Dem erläuternden Bericht ist insoweit zuzustimmen, als diese Begrenzung für Gerichtsverfahren, in denen die Parteien lediglich Dokumente im PDF-Format einreichen, bei weitem ausreichen wird.

Bereits heute kommt es jedoch vor, dass insbesondere in Strafverfahren Beweismittel vorhanden sind, welche diese Grössenbeschränkung deutlich überschreiten. Es dürfte dem Publikum schwer vermittelbar sein, wenn solche oftmals ausschliesslich in digitaler Form vorliegenden Beweismittel nicht über die Plattform übermittelt werden könnten und stattdessen andere Wege gefunden werden müssten, um diese zu den Akten zu nehmen und den Parteien Einsicht zu gewähren.

Dies gilt umso mehr, als dem Publikum seit Jahren kommuniziert wird, dass die Justiz mit der Einführung der elektronischen Kommunikation über die Plattform und der digitalen

Aktenführung im digitalen Zeitalter angekommen ist. Hinzu kommt, dass die Digitalisierung zunehmend alle Lebensbereiche durchdringt und rasch voranschreitet. Es ist absehbar, dass die Gerichte künftig deutlich häufiger als heute mit digitalen Beweismitteln mit grossem Datenvolumen konfrontiert sein werden.

Art. 5: Quittung

Art. 5 Abs. 2 Bst. b hält fest, dass die Quittung gegebenenfalls den Namen oder die Firma der Organisation enthalten muss, für welche die Absenderin oder der Absender handelt.

Diese Bestimmung ist nicht klar. Ein Rechtsanwalt kann vor Gericht eine juristische Person vertreten und handelt entsprechend für diese juristische Person. Ist die Bestimmung dahingehend zu verstehen, dass in einem solchen Fall der Name oder die Firma dieser juristischen Person, d. h. der Klientin oder des Klienten des Rechtsanwalts, auf der Quittung erscheinen soll?

Sollte mit «Organisation» hingegen die Anwaltskanzlei gemeint sein, welcher der Rechtsanwalt angehört, stellt sich die Frage, ob der Rechtsanwalt in einem Gerichtsprozess tatsächlich für die Anwaltskanzlei handelt, da er in Vertretung seiner Mandantschaft auftritt. Zudem kann es vorkommen, dass die Mandantschaft lediglich dem prozessführenden Rechtsanwalt eine Vollmacht erteilt hat. Dies gilt insbesondere deshalb, weil zahlreiche Anwaltskanzleien als reine Unkostengemeinschaften organisiert sind und die einzelnen Rechtsanwältinnen und Rechtsanwälte ihre Mandate eigenständig führen.

Art. 9: Profile

Art. 9 Abs. 4 besagt, dass die Profile von natürlichen Personen, die zur elektronischen Übermittlung verpflichtet und für eine Organisation tätig sind, zusätzlich zu den Angaben nach Abs. 3 Bst. a den Namen oder die Firma der Organisation enthalten müssen.

Im erläuternden Bericht wird ausgeführt, dass Organisationen im Sinne von Abs. 4 juristische Personen, aber auch andere Organisationsformen wie einfache Gesellschaften oder Kollektivgesellschaften sein können. Insbesondere Anwaltskanzleien seien häufig in einer solchen Rechtsform organisiert.

Die Bestimmung von Art. 9 Abs. 4 ist unklar. Im Gerichtsverfahren ist ein Rechtsanwalt für die Mandantschaft tätig, die ihn entsprechend bevollmächtigt hat, und nicht für die Kanzlei. Hinzu kommt, dass viele Anwaltskanzleien als Unkostengemeinschaften strukturiert sind und der Rechtsanwalt daher auch in diesem Sinne nicht für die «Organisation» vor Gericht tätig ist. Gerade in solchen Konstellationen kommt es vor, dass die Mandantschaft lediglich den prozessführenden Rechtsanwalt mandatiert hat und nicht auch die auf eigene Rechnung tätigen Büropartner.

Art. 14: Virenprüfung

Abs. 1 sieht vor, dass die Plattform nur für Dokumente bis zu 64 Megabyte eine Virenprüfung durchführen muss. Bei grösseren Dokumenten wird es gemäss Abs. 2 der Plattform überlassen, ob sie auf eine Virenprüfung verzichtet oder die Dokumente in 64 Megabyte grosse Teile aufteilt und diese einer Virenprüfung unterzieht.

Mangels einer vollständigen Virenprüfung durch die Plattform müssen die Kantone eine eigene Virenprüfung vorsehen. Dadurch entstehen Doppelspurigkeiten, die vermieden werden sollten.

Art. 16: Aufteilung der Gebühr

Abs. 2 besagt, dass der Anteil der Kantone gemäss der im Zeitpunkt der Festlegung der Gebühr massgebenden Wohnbevölkerung auf die an der Vereinbarung beteiligten Kantone aufgeteilt wird.

Das Ausmass der Nutzung der Plattform kann auch nach der schweizweiten Geltung des Obligatoriums je nach Kanton sehr unterschiedlich ausfallen. Dies hängt insbesondere davon ab, ob die Aktenübermittlung zwischen Behörden kantonsintern über die Plattform oder über ein anderes kantonales System erfolgt. Aus diesem Grund sollte die Kostenverteilung auf der effektiven Nutzung basieren, wie dies in der verworfenen Variante vorgesehen war.

Im erläuternden Bericht wird die Kostenverteilung aufgrund der effektiven Nutzung mit dem Argument verworfen, dass die effektive Nutzung bis zur schweizweiten Geltung des Obligatoriums je nachdem, zu welchem Zeitpunkt ein Kanton das Obligatorium einführt, sehr unterschiedlich ausfallen könne. Dadurch würden jene Kantone, welche frühzeitig das Obligatorium umsetzen, übermässig belastet.

Diesem Bedenken kann jedoch begegnet werden, indem der Kantonsanteil während der Übergangsphase bis zur gesamtschweizerischen Einführung des Obligatoriums nach Massgabe der Wohnbevölkerung verteilt wird und erst danach auf die effektive Nutzung abgestellt wird.

Art. 23: Eignungsvoraussetzungen

Die vorgeschlagenen Ausführungsbestimmungen orientieren sich stark an der technischen Lösung der zentralen Plattform. Für die elektronische Weitergabe innerhalb eines Kantons (ZPO) oder zwischen Strafbehörden (StPO) sollten jedoch andere Anforderungen gelten als für die Kommunikation über die zentrale Plattform.

Die elektronische Weitergabe innerhalb eines Kantons kann künftig beispielsweise durch die Mutation von Zugriffsrechten auf einer gemeinsamen kantonalen Datenbank erfolgen, was in den Logfiles des kantonalen IT-Systems protokolliert wird. Für solche Fälle erscheint ein synchronisierter Zeitstempel, wie er in Art. 23 Bst. b vorgeschrieben ist, als unnötig.

Zur Klarstellung sollte Art. 23 dahingehend ergänzt werden, dass die elektronische Weitergabe von Dokumenten durch Mutation von Zugriffsrechten auf einer gemeinsamen Datenbank zulässig ist.

Art. 24: Elektronische Übermittlung unter Behörden

Art. 24 stellt strengere Anforderungen als Art. 23, ohne dass hierfür ein sachlicher Grund ersichtlich ist. Aus unserer Sicht sollten sich die Voraussetzungen für die elektronische Übermittlung unter Behörden nach Art. 24 an jenen von Art. 23 orientieren und nicht darüber hinausgehen.

Freundliche Grüsse

Die Obergerichtspräsidentin

Dr. iur. Petra Hauser

Der Generalsekretär

lic. iur. Erich Hug