



Bern, 13. März 2026

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

Erläuternder Bericht
zur Eröffnung
des Vernehmlassungsverfahrens



Übersicht

Ausgangslage

Am 20. Dezember 2024 hat die Bundesversammlung das Bundesgesetz über die Plattformen für die elektronische Kommunikation (BEKJ) verabschiedet (BBl 2025 19, AS 2025 583). Mit diesem Gesetz wird ein Obligatorium zur elektronischen Kommunikation für die professionellen Rechtsanwenderinnen und -anwender eingeführt. Das Obligatorium betrifft insbesondere die Behörden einschliesslich der Gerichte und der Staatsanwaltschaften sowie die Anwaltschaft. Der Bund und die Kantone können für ihre Verfahren das Obligatorium während einer Übergangsfrist von fünf Jahren variabel einführen. Ebenfalls soll eine öffentlich-rechtliche Körperschaft gegründet werden, welche für den Aufbau, Betrieb und Weiterentwicklung der zentralen Plattform zuständig ist. Über diese erfolgt die elektronische Kommunikation in Zivil- und Strafverfahren sowie in der Verwaltungsgerichtsbarkeit. Für die Verwaltungsverfahren des Bundes sieht das BEKJ vor, dass eine Verwaltungseinheit der zentralen Bundesverwaltung eine Plattform bereitstellt.

Die Referendumsfrist zum BEKJ ist am 19. April 2025 ungenutzt abgelaufen. Am 1. Oktober 2025 ist eine erste Teilkraftsetzung des BEKJ¹ erfolgt. Für die abschliessende Inkraftsetzung des BEKJ müssen verschiedene Voraussetzungen erfüllt sein:

- Die Gründung der Körperschaft justitia.swiss (Bund und mindestens achtzehn Kantone),*
- die Bewilligung und Inbetriebnahme der Plattform justitia.swiss,*
- die Erreichbarkeit sämtlicher vom BEKJ erfassten Gerichte des Bundes und der Kantone auf einer Plattform,*
- die Verabschiedung der Ausführungsbestimmungen zum BEKJ.*

Es wird davon ausgegangen, dass diese Voraussetzungen frühestens am 1. Januar 2027 erfüllt sein werden.

Inhalt der Vorlage

Die Vorlage enthält insbesondere Bestimmungen betreffend Erteilung einer Betriebsbewilligung an die Plattformen nach dem BEKJ, dem Authentifizierungsmittel für die Benutzung der Plattformen, den zugelassenen Dokumentenformaten und -grössen sowie der Gebührenhöhe und deren Erhebung.

¹ SR 172.023

Inhaltsverzeichnis

1	Ausgangslage	4
2	Grundzüge der Vorlage	5
2.1	Betriebsbewilligung	5
2.2	Authentifizierungsmittel	6
2.3	Zugelassene Formate und Grösse der Dokumente.....	6
2.4	Digitalisierung von papiernen Eingaben	6
2.5	Gebühren	7
2.6	Verworfenne Regulierungsideen	7
3	Erläuterungen zu einzelnen Artikeln	9
4	Erläuterungen zu Anhang 1 (Aufhebung und Änderung anderer Erlasse).35	
4.1	Aufhebung der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV).....	35
4.2	Aufhebung der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV)	35
4.3	Verordnung vom 23. November 2016 über die elektronische Signatur ...	36
5	Erläuterungen zu Artikel 26 Absatz 5 BEKJ	37
6	Auswirkungen	38
6.1	Auswirkungen auf den Bund.....	38
6.2	Auswirkungen auf Kantone und Gemeinden	38
6.3	Auswirkungen auf die Volkswirtschaft	38
6.4	Auswirkungen auf die Gesellschaft	39
7	Rechtliche Aspekte	39
7.1	Informationssicherheit	39
7.2	Datenschutz	40

Erläuternder Bericht

1 Ausgangslage

Am 20. Dezember 2024 hat die Bundesversammlung das Bundesgesetz über die Plattformen für die elektronische Kommunikation (BEKJ) verabschiedet (BBl 2025 19, AS 2025 583). Mit diesem Gesetz wird ein Obligatorium zur elektronischen Kommunikation für die professionellen Rechtsanwenderinnen und -anwender eingeführt. Das Obligatorium betrifft insbesondere die Behörden einschliesslich der Gerichte und der Staatsanwaltschaften sowie die Anwaltschaft. Der Bund und die Kantone können für ihre Verfahren das Obligatorium während einer Übergangsfrist von fünf Jahren variabel in Kraft setzen. Ebenfalls soll eine öffentlich-rechtliche Körperschaft gegründet werden, welche für den Aufbau, Betrieb und Weiterentwicklung einer zentralen Plattform zuständig ist. Über diese erfolgt die elektronische Kommunikation in Zivil- und Strafverfahren sowie in der Verwaltungsgerichtsbarkeit. Für die Verwaltungsverfahren des Bundes sieht das BEKJ vor, dass eine Verwaltungseinheit der zentralen Bundesverwaltung eine Plattform bereitstellt.

Die Referendumsfrist zum BEKJ ist am 19. April 2025 ungenutzt abgelaufen. Am 19. September 2025 hat der Bundesrat beschlossen jenen Teil des BEKJ auf den 1. Oktober 2025 in Kraft zu setzen, welcher für die Schaffung der zentralen BEKJ-Plattform nötig ist (insb. Art. 1–17 BEKJ). Für die abschliessende Inkraftsetzung des BEKJ müssen verschiedene Voraussetzungen erfüllt sein:

- Die Gründung der Körperschaft justitia.swiss (Bund und mindestens achtzehn Kantone),
- die Bewilligung und Inbetriebnahme der Plattform justitia.swiss,
- die Erreichbarkeit sämtlicher vom BEKJ erfassten Gerichte des Bundes und der Kantone auf einer Plattform,
- die Verabschiedung der Ausführungsbestimmungen zum BEKJ.

Es wird davon ausgegangen, dass diese Voraussetzungen frühestens am 1. Januar 2027 erfüllt sein werden.

Um die zentrale Plattform bereits frühzeitig testen zu können, wurden basierend auf den bestehenden Bestimmungen über den elektronischen Rechtsverkehr verschiedene Pilotprojekte nach Artikel 13a der Verordnung vom 18. Juni 2010² über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV) bewilligt. Diese Pilotprojekte haben wertvolle Erkenntnisse geliefert und haben dazu beigetragen, dass die zentrale Plattform gemäss den Anforderungen optimiert für die Benutzerinnen und Benutzer für den betrieblichen Einsatz bereitsteht. Es traten keine nennenswerten Probleme auf.

² SR 272.1

2 Grundzüge der Vorlage

Mit dem BEKJ hat das Parlament die Grundlagen geschaffen, um durchgängig digitale, medienbruchfreie Justizverfahren zu ermöglichen. Die Aktenführung erfolgt elektronisch. Für professionelle Rechtsanwenderinnen und -anwender, insbesondere Gerichte, Behörden und Anwaltschaft, wird die Kommunikation auf diesem Weg zur Pflicht. Der vorliegende Vorentwurf der Verordnung über die elektronische Kommunikation in bundesrechtlichen Justiz- und Verwaltungsverfahren (nachfolgend: VE-VEKJ) dient hauptsächlich der Umsetzung des BEKJ. Er konkretisiert die Voraussetzungen für eine Betriebsbewilligung sowie das Bewilligungsverfahren für die Plattformen nach dem BEKJ. Zudem regelt der VE-VEKJ, die zugelassenen Authentifizierungsmittel, die zulässigen Formate für die Übermittlung und deren Grösse, das elektronische Einlesen von papiernen Eingaben auf Seite der Gerichte und Behörden sowie die Gebühren. Daneben übernimmt er einzelne Bestimmungen des eSchKG³, die bisher in der VeÜ-ZSSV standen. Die VeÜ-ZSSV wird mit der abschliessenden Inkraftsetzung des BEKJ aufgehoben. Zudem passt der VE-VEKJ die Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES)⁴ an.

Der VE-VEKJ gilt für alle dem BEKJ unterstehenden Plattformen, insbesondere auch für die zukünftige Plattform für die Verwaltungsverfahren des Bundes sowie für die elektronische Übermittlung im Bereich des SchKG. Der technische Rahmen der zukünftigen Plattform des Bundes ist aktuell noch nicht bekannt. 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. Dies gilt insbesondere für die Regelung der mit der Benutzung der Plattform verbundenen bundesverwaltungs-internen Verteilung der Kosten.

Um die Praxistauglichkeit zu gewährleisten, wurde eine Begleitgruppe einberufen bestehend aus Vertreterinnen und Vertretern der Bundesverwaltung, des Bundes- und Bundesverwaltungsgerichts, der Bundesanwaltschaft, kantonalen Gerichten und Staatsanwaltschaften sowie dem schweizerischen Anwaltsverband.

2.1 Betriebsbewilligung

Zusätzlich zu der zentralen Plattform der öffentlich-rechtlichen Körperschaft und der allgemeinen Plattform für Verwaltungsverfahren des Bundes können die Kantone

³ Beim eSchKG handelt es sich um einen Standard für den Austausch von elektronischen Betreibungsdaten zwischen natürlichen Personen, juristischen Personen des privaten und des öffentlichen Rechts sowie Betreibungsämtern. Für weitere Informationen siehe www.eschkg.ch.

⁴ SR 943.032

noch weitere Plattformen nach dem BEKJ entwickeln. Der Betrieb dieser Plattformen muss nach Artikel 25 BEKJ vom EJPD bewilligt werden.

Für die Bewilligung müssen verschiedene Anforderungen bezüglich der eingesetzten Kryptographie und Schlüsselverwaltung, Quittungen, Datenschutz und Datensicherheit sowie Schnittstellen erfüllt werden. Teilweise ergeben sich die Bewilligungsvoraussetzungen bereits aus dem BEKJ selbst, teilweise aus dem VE-VEKJ. Schliesslich wird das EJPD im VE-VEKJ mit der Aufgabe betraut, die funktionalen und betrieblichen Anforderungen an die Plattformen in einer Departementsverordnung sowie die technischen Vorgaben und das Datenformat der Schnittstellen zu regeln.

Das EJPD wird im Rahmen der Umsetzung prüfen, ob es sinnvoll ist, ein Merkblatt zu erarbeiten, welches sämtliche Bewilligungsvoraussetzungen detailliert zusammenfasst.

2.2 Authentifizierungsmittel

Der VE-VEKJ sieht vor, dass als Authentifizierungsmittel grundsätzlich das Behörden-Login AGOV verwendet wird. AGOV ermöglicht unter anderem, dass auch Personen im Ausland ein solches Login erhalten können. Voraussetzung ist ein gültiger Reisepass oder eine Identitätskarte.

2.3 Zugelassene Formate und Grösse der Dokumente

Der VE-VEKJ unterscheidet zwischen Mitteilungen der Behörden, Eingaben der übrigen Verfahrensparteien und den Beilagen von allen an einem Verfahren beteiligten Behörden und Parteien. Für die Mitteilungen seitens der Behörden ist das Format PDF/A vorgeschrieben, wobei sämtliche ISO-konforme Varianten (PDF/A-1 bis PDF/A-4) zulässig sind. Die übrigen Verfahrensparteien können ihre Einlagen im Format PDF oder PDF/A übermitteln. Die Beilagen können in jeglichem Format übermittelt werden. Kann die Behörde das Format nicht öffnen, kann die Nachsendung in einem für die Behörde lesbaren Format verlangt werden. Der VE-VEKJ sieht eine Liste von Formaten vor, welche die verfahrensleitende Behörde öffnen können muss.

Es ist eine Grössenbeschränkung von 2 Gigabyte pro Dokument vorgesehen. Dies dürfte für einen Grossteil der übermittelten Dokumente ausreichend sein. Diese Grenze ist deutlich höher als im heutigen elektronischen Rechtsverkehr über die anerkannten Zustellplattformen. Dort beträgt die effektive Nutzgrösse pro Sendung nur 15 Megabyte. Sollte ein Dokument ausnahmsweise grösser als 2 Gigabyte sein, lässt es sich in kleinere Dateien aufteilen.

2.4 Digitalisierung von papiernen Eingaben

Der VE-VEKJ gibt eine Mindestqualität vor, die beim Einlesen von papiernen Dokumenten in elektronische Dokumente beachtet werden muss. Darüber hinaus verpflichtet der VE-VEKJ die Behörden zur Qualitätskontrolle der digitalisierten Dokumente.

2.5 Gebühren

Der VE-VEKJ sieht die Erhebung von pauschalen Gebühren pro Kanton und für den Bund vor. Der Bund wird einen Anteil von 10 % übernehmen. Die restlichen Gebühren verteilt sich gemäss Einwohnerzahl auf die Kantone.

Als Grundlage für die Gebührenhöhe dient die Finanzplanung der öffentlich-rechtlichen Körperschaft. Die Körperschaft wird bei der Finanzplanung auch Unvorhergesehenes berücksichtigen müssen. Um die Liquidität zu gewährleisten, kann eine Reserve von 10 % der jährlichen Gesamtkosten gebildet werden.

2.6 Verworfenne Regulierungsideen

Rücksendung von Dokumenten

In den Diskussionen der Begleitgruppe wurde angeregt eine Verordnungsbestimmung zu schaffen, wonach gewisse physisch eingereichte Dokumente nicht zurückgesendet werden müssen. Konkret geht es um Dokumente, die speziell für Behörden geschrieben wurden (z. B. Strafanzeigen) und somit in digitaler Form bei der Urheberschaft vorhanden sind oder es sich um Kopien von rechtsrelevanten Dokumenten handelt, deren Originale bei den Personen, die eine Eingabe machen, verbleiben.

Dieser Vorschlag wurde verworfen, weil aufgrund von Artikel 30 BEKJ kein Handlungsspielraum verbleibt, um auf Verordnungsstufe einen Teil der physisch eingereichten Dokumente nicht zurückzusenden.

Versand in Papierform

In den Diskussionen der Begleitgruppe wurde angeregt, dass anstelle eines eigenhändig unterschriebenen Entscheids ein Ausdruck des elektronischen Originals an Personen versendet werden könnte, die nicht elektronisch mit dem Gericht oder der Behörde kommunizieren. Insbesondere hiess es, dass die Verfahrensgesetze nicht vorsehen, dass die Unterschriften der Behördenmitglieder handschriftlich sein müssen.

Im Anhang der Änderung der anderen Erlasse zum BEKJ wurden alle Gesetzesbestimmungen, in welchen bisher eine Unterschrift seitens Behörde oder Gericht verlangt wird, mit dem Einschub «falls der Entscheid auf Papier versendet wird» oder ähnlich ergänzt (siehe beispielsweise Art. 238 Bst. h Zivilprozessordnung⁵ [ZPO], Art. 353 Abs. 1 Bst. k Strafprozessordnung⁶ [StPO], Art. 153 Abs. 3 Militärstrafprozess

⁵ SR 272

⁶ SR 312.0

vom 23. März 1979⁷). Mit dem BEKJ wird folglich explizit geregelt, dass eine Unterschrift bei Papierversand notwendig ist. Eine qualifizierte elektronische Signatur, verbunden mit einem qualifizierten Zeitstempel gemäss dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderen Anwendungen digitaler Zertifikate vom 18. März 2016⁸ (ZertES), ist zwar der eigenhändigen Unterschrift gleichgestellt (Artikel 14 Abs. 2^{bis} Obligationenrecht⁹ [OR]). Diese Signatur und der Zeitstempel können jedoch nicht formerhaltend auf Papier ausgedruckt werden. Für eine abweichende Regelung auf Verordnungsstufe verbleibt kein Spielraum.

Übergangsbestimmung Weiternutzung von IncaMail und PrivaSphere

In den Diskussionen der Begleitgruppe wurde auch das Bedürfnis genannt, Übergangsbestimmungen zu schaffen, die die Weiterverwendung der bisherigen anerkannten Zustellplattformen für eine begrenzte Zeitdauer erlauben würden.

Dies ist nicht möglich, da die gesetzlichen Grundlagen der bisherigen Übermittlungsverordnungen in den Verfahrensgesetzen mit der abschliessenden Inkraftsetzung wegfallen. Auf dem Verordnungsweg kann das Fehlen der gesetzlichen Grundlagen mittels Übergangsbestimmungen nicht übersteuert werden; hierzu würden Übergangsrechtliche Bestimmungen auf Gesetzesstufe benötigt.

Allerdings ist darauf hinzuweisen, dass im Rahmen der bei abschliessender Inkraftsetzung hängigen Verfahren die bisherigen anerkannten Zustellplattformen weiterhin benutzt werden können. Die Prozessgesetze enthalten entsprechende Übergangsbestimmungen, wonach bei hängigen Verfahren das bisherige Recht weiter anwendbar ist. Dies gilt auch für die elektronische Übermittlung mittels der heute anerkannten Zustellplattformen. Für neue Verfahren ist hingegen eine Plattform nach dem BEKJ zu verwenden.

Zudem können die bisherigen anerkannten Zustellplattformen im Rahmen von Artikel 6a Absatz 4 VwVG weiterverwendet werden.

Aufgrund des Berechtigungssystems gemäss Artikel 24 BEKJ ist folgendes Vorgehen ebenfalls denkbar: Die bisher anerkannten Zustellplattformen können ein Organisationskonto auf der Plattform eröffnen. Benutzerinnen und Benutzer, die weiterhin die bisher anerkannten Zustellplattformen benutzen wollen, können der von ihnen benutzten Zustellplattform Berechtigungen zur Übermittlung und zum Abruf erteilen. Die bisherigen Benutzerinnen und Benutzer können weiterhin eine der heute anerkannten Zustellplattformen benutzen und müssen ihren Geschäftsablauf nicht ändern. Einzig

⁷ SR 322.1

⁸ SR 943.03

⁹ SR 220

wenn es sich bei der Benutzerin um eine Behörde handelt, muss anstelle der qualifizierten elektronischen Signatur ein geregeltes elektronisches Siegel (vgl. Artikel 22 Absatz 2 BEKJ) verwendet werden.

3 Erläuterungen zu einzelnen Artikeln

Ingress

Mit dem BEKJ wird eine Reihe von Verfahrensgesetzen geändert, was zu einer hohen Anzahl an Delegationsnormen führt. Um die Übersichtlichkeit im Ingress zu bewahren, wird das BEKJ als Ganzes, nicht aber die einzelnen Delegationsnormen aufgeführt. Zusätzlich werden diejenigen Bestimmungen aus anderen Verfahrensgesetzen aufgeführt, die die Kommunikation ausserhalb der BEKJ-Plattformen zum Inhalt haben und somit den Geltungsbereich des VE-VEKJ erweitern.

1. Kapitel: Betrieb und Nutzung von Plattformen

1. Abschnitt: Geltungsbereich

Art. 1

Abs. 1

Diese Bestimmung definiert den Geltungsbereich des 1. Kapitels des VE-VEKJ. Sie legt dar, auf welche Plattformen und Verfahren die nachfolgenden detaillierten Regelungen insbesondere zum Betrieb, zur Nutzung, zu den technischen und organisatorischen Anforderungen, Anwendung finden. Für die in Absatz 1 aufgeführten Plattformen gelten diese Regelungen zwingend.

Abs. 2

Die Regelungen des 1. Kapitels gelten auch für andere, spezialgesetzlich geregelte Plattformen, soweit das BEKJ auf diese Plattformen und Verfahren überhaupt Anwendung findet. Viele Spezialgesetze verweisen bereits heute auf das Verwaltungsverfahrensgesetz vom 20. Dezember 1968 (VwVG)¹⁰ und damit indirekt auf elektronische Kommunikationsmöglichkeiten. Wenn und soweit diese Verweise durch die BEKJ-Anpassungen auch die Plattform(en) nach BEKJ erfassen, dann unterstehen auch diese Spezialplattformen den Vorgaben des 1. Kapitels.

Abs. 3

Dieser Absatz regelt, dass spezifischere Regelungen in anderen Bundesgesetzen bzw. deren Verordnungen dem VEKJ vorgehen werden, soweit sie davon abweichen.

¹⁰ SR 172.021

2. Abschnitt: Betriebsbewilligung

Art. 2 Anforderungen an die Plattformen

Abs. 1

Dieser Absatz regelt die Voraussetzungen für eine Betriebsbewilligung einer Plattform nach dem BEKJ. Im BEKJ sind insbesondere auch Anforderungen an die Plattformen bezüglich des Datenschutzes und der Datensicherheit enthalten (siehe Artikel 27 f. BEKJ). Neben den Anforderungen des BEKJ müssen die Plattformen zusätzliche Vorgaben erfüllen, die im Folgenden erläutert werden.

Bst. a

Aufgrund von datenschutzrechtlichen Vorgaben (Art. 8 Abs. 1 des Datenschutzgesetzes vom 25. September 2020 [DSG]¹¹) und auch um das Vertrauen der Bevölkerung in die Justiz aufrechtzuerhalten, müssen die Plattformen die bei ihnen gespeicherten Dokumente so sichern, dass Unbefugte weder darauf zugreifen noch sie verändern können. Dies umfasst technische Massnahmen wie Verschlüsselung, Zugriffssteuerung und Protokollierung von Zugriffen und Zugriffsversuchen. Bezüglich der Verschlüsselung während der Übermittlung siehe die Erläuterungen zu Buchstabe b.

Weiter müssen die Plattformen Angriffe wie Hackingversuche oder Manipulation abwehren können. Ohne solche Abwehrmechanismen könnten der Datenschutz und der informationssicherheitsrechtliche Schutz nicht gewährleistet werden. Die Plattformen müssen potenzielle Angriffe erkennen und blockieren können, um Vertraulichkeit (kein Zugriff für Unbefugte) und Integrität (keine unbefugten Änderungen) zu sichern.

Bst. b

Die Verschlüsselung der Daten muss den Standards der Bundesverwaltung entsprechen. Dies bedeutet, dass Algorithmen wie AES-256 oder vergleichbare/neuere Methoden verwendet werden müssen, um Daten während der Übertragung und Speicherung zu schützen. Dies stellt sicher, dass der elektronische Rechtsverkehr den hohen Sicherheitsanforderungen genügt und mit internationalen Normen kompatibel ist.

Die Plattformen müssen in der Lage sein, Kommunikation gemäss den Standards der Bundesverwaltung für sichere Übermittlung durchzuführen. Effektiv bezieht sich das auf Protokolle wie HTTPS oder TLS, die eine sichere Datenübertragung garantieren. Eine Übersicht dieser Standards findet sich unter: [bk.admin.ch > Digitale Transformation und IKT-Lenkung > Vorgaben](https://www.bk.admin.ch/bk/inf/04833/index.html).

¹¹ SR 235.1

Bst. c

Die Plattformen müssen Dokumente bis zu einer Grösse von 2 Gigabyte entgegennehmen und übermitteln können. Diese Beschränkung sollte in den allermeisten Fällen ausreichend sein. Textdokumente und Tabellenkalkulationen werden diese Grösse schwerlich erreichen, ausser sie enthalten eingebettete Medien. Auch Fotos mit aktuellen Mobiltelefonen oder Digitalkameras werden dieses Limit kaum erreichen. Lediglich aktuelle Digitalkameras mit der Einstellung, dass die Fotos im Rohformat gespeichert werden, sowie Videos können dieses Limit von 2 Gigabyte überschreiten.

Der heutige E-Mail-basierte Rechtsverkehr lässt pro Eingabe nur eine Nutzgrösse von 15 Megabyte zu. Damit sind die 2 Gigabyte pro Dokument erheblich grosszügiger und ausreichend. Zudem lassen sich Dokumente ohne Probleme auch in mehrere Teile aufspalten. So können Videodateien ohne Probleme in Teile aufgeteilt werden, die wiederum Videodateien sind. Für andere Formate ist möglicherweise der Beizug einer Archivierungssoftware wie Zip und 7-Zip notwendig, um die Dokumente aufspalten zu können.

Die Betreiberinnen von Plattformen können in die Übermittlung von grösseren Dokumenten einwilligen. Abbilder von beschlagnahmten Computern und Mobiltelefone werden in der Regel die Grösse von 2 Gigabyte pro Dokument überschreiten. Die beschlagnahmten Geräte werden beispielsweise durch forensische Labors ausgewertet und dann den jeweiligen Strafverfolgungsbehörden übermittelt. Die übermittelten Datenmengen können hunderte von Gigabytes oder gar Terabytes betragen.

Die Standardübermittlung über die Plattformen ist nicht auf diese speziellen Fälle ausgelegt, dennoch sollen auch diese Daten übermittelt werden können. Damit solche Abbilder und Dateien übermittelt werden können, ohne in mehrere Teile aufgespalten zu werden, können die Betreiberinnen von Plattformen auch die Übermittlung von grösseren Dokumenten durch spezifische Benutzerinnen und Benutzer zulassen.

Die Einwilligung kann mündlich oder schriftlich erfolgen, sie kann auch unter Vorbehalt von Haftungsausschlüssen etc. erteilt werden. In der Regel wird die Einwilligung schriftlich erfolgen, kann aber in dringenden Fällen vorab mündlich erteilt werden.

Alternativ kann auch der Zugriff auf eine forensische Applikation erlaubt werden, um dadurch auf die Beilage zugreifen zu können.

Bst. d

Die Plattformen müssen es den Benutzerinnen und Benutzern ermöglichen, Dokumente jederzeit aus ihrem Profil zu entfernen. Dies kann insbesondere für die Benutzerinnen und Benutzer wichtig sein, die die Benutzeroberfläche nach Artikel 19 Absatz 1 BEKJ benutzen und ihren Eingang/Ausgang aufräumen möchten. Das Entfernen aus dem Profil hat nicht unbedingt die Löschung auf der Plattform zu Folge. Technisch gesehen erfolgt die Löschung wie folgt: Ein Dokument wird beispielsweise von einer Behörde an mehrere Verfahrensbeteiligte übermittelt. Das Dokument wird

nur einmal auf der zentralen Plattform gespeichert und den jeweiligen Empfängerinnen und Empfängern sowie der zustellenden Behörde eine Berechtigung zugeteilt. Solange noch weitere Parteien die Berechtigung haben, bewirkt das Entfernen durch eine Partei aus ihrem Profil lediglich den Entzug der Berechtigung. Diese Partei kann danach nicht mehr auf das Dokument zugreifen. Die physische Löschung erfolgt erst, sobald alle Berechtigungen (automatisch oder manuell) entzogen sind.

Abs. 2

Zusätzlich regelt Absatz 2, dass das EJPD die funktionalen und betrieblichen Anforderungen an die Plattformen, einschliesslich der Schnittstellen, im Rahmen der bundesrätlichen Vollzugskompetenz konkretisiert. Der genaue Umfang der Delegation an das EJPD wird während des Vernehmlassungsverfahrens konkretisiert.

Die Plattformen müssen Schnittstellen bereitstellen, über die andere Programme mit den Plattformen kommunizieren können. So können Dritte ihre speziellen Anwendungen (z.B. Geschäftsverwaltungssoftware) ohne Extrakosten mit den Plattformen verbinden. Durch solche Verbindungen lassen sich Dokumente automatisch übermitteln oder von den Plattformen abrufen. Besonders für professionelle Benutzerinnen und Benutzer, die mehrmals täglich Dokumente übermitteln oder abrufen, ist diese Anbindung wichtig. Sie hilft, die Geschäftsabläufe zu optimieren und den Rechtsverkehr mit den Behörden zu vereinfachen. Die Schnittstellen der zentralen Plattform sowie der Plattform nach Artikel 6a Absatz 2 VwVG sind kostenlos benutzbar. Dies soll die Akzeptanz der Plattformen in der Praxis erhöhen.

Um den sicheren und interoperablen elektronischen Rechtsverkehr zu gewährleisten, erlässt das EJPD technische Vorgaben zu Protokollen (etwa RESTful APIs, SOAP oder spezifische Sicherheitsstandards wie TLS 1.3), Leistungsanforderungen (z. B. Antwortzeiten) oder Integrationsrichtlinien. Das stellt sicher, dass die Schnittstellen robust, skalierbar und widerstandsfähig gegen Störungen sind. Ebenfalls bestimmt das EJPD das Datenformat der Übermittlung wie beispielsweise XML oder JSON.

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). Die zentrale Plattform muss ihre Schnittstellen kostenlos bereitstellen. Dies entspricht der Regelung von Artikel 32 Absatz 1 BEKJ. Dieser Artikel sieht vor, dass die Körperschaft nur Gebühren von den Behörden erhebt. In der Botschaft¹² zum BEKJ wurde im hier relevanten Kontext in Ziffer 4.2.2.4 explizit hervorgehoben, dass keine Bezahlschranken für die Benutzerinnen und Benutzer errichtet werden sollen.

Das EJPD wird prüfen, ob es sinnvoll ist, ein Merkblatt mit allen Bewilligungsvoraussetzungen und Prüfungspunkten zu veröffentlichen. Dieses könnte die Betreiberinnen

¹² BBl 2023 679

von Plattformen beim Verfassen des Gesuchs und Zusammentragen der notwendigen Unterlagen unterstützen.

Art. 3 Bewilligungsverfahren

Abs. 1 und 2

Das EJPD ist für das Bewilligungsverfahren von Plattformen nach dem BEKJ zuständig. Diese Lösung hat sich in der Praxis bewährt, da das EJPD bereits heute für das Bewilligungsverfahren von Zustellplattformen verantwortlich ist und zudem das federführende Departement für Gesetzgebungsarbeiten im Bereich des BEKJ ist. Wer eine Plattform nach dem BEKJ betreiben möchte, muss dem EJPD ein Gesuch einreichen. In diesem Gesuch muss die gesuchstellende Betreiberin nachweisen, dass sie alle Voraussetzungen erfüllt. Dazu gehören insbesondere:

- Ein Konzept, das belegt, dass sämtliche Bewilligungsvoraussetzungen erfüllt sind;
- Unterlagen zu den technischen Spezifikationen der Plattform;
- Sicherheitszertifikate, die die Einhaltung der gesetzlichen Anforderungen nachweisen; und
- Angaben zur Unternehmensstruktur der Gesuchstellerin.

Diese Anforderungen dienen dazu, sicherzustellen, dass nur Plattformen eine Bewilligung erhalten, die den hohen Standards des BEKJ entsprechen und somit den Schutz der Nutzerinnen und Nutzer sowie die Integrität des elektronischen Rechtsverkehrs gewährleisten können.

Abs. 3

Das EJPD wird verpflichtet, die Einzelheiten des Bewilligungsverfahrens in einer Departementsverordnung zu regeln. Dabei hat es insbesondere festzulegen, welche Angaben mit dem Gesuch einzureichen sind. Der Inhalt dieser Departementsverordnung wird während des Vernehmlassungsverfahrens ausgearbeitet.

Abs. 4

Aufgrund des Fortschritts und der stetigen Änderung der Bedrohungslage im digitalen Bereich muss durch die Bewilligungsinstanz regelmässig geprüft werden, ob eine Plattform die Voraussetzungen zum Erhalt einer Bewilligung weiterhin erfüllt. Ist dies nicht mehr der Fall, dann muss als ultima ratio eine erteilte Bewilligung entzogen werden. Dies ist notwendig, um den Schutz der Nutzerinnen und Nutzer sowie die Integrität und das Vertrauen in den elektronischen Rechtsverkehr zu wahren. Der Entzug soll jedoch nicht leichtfertig erfolgen. Insbesondere kann das EJPD im Sinn einer milderen Massnahme eine Frist zur Wiederherstellung des gesetzmässigen Zustands ansetzen, mit der Androhung, dass bei Missachten der Frist die Bewilligung entzogen wird.

Wird einer Plattform die Bewilligung als ultima ratio entzogen, so werden die betroffenen Kantone, die die Plattform benutzen, sich einer anderen bewilligten Plattform anschliessen müssen. Dies muss umgehend erfolgen, damit mit Behörden der betroffenen Kantone weiterhin elektronisch kommuniziert werden kann. Dem Bund sind keine Bestrebungen bekannt, dass weitere Plattformen nach Artikel 4 BEKJ entwickelt werden.

Abs. 5

Für die Prüfung eines Gesuchs und der Erteilung der Bewilligung wird ein Stundenansatz von 250 Franken verrechnet. Zusätzlich sind die Bestimmungen der Allgemeinen Gebührenverordnung vom 8. September 2004 (AllGebV)¹³ anwendbar.

3. Abschnitt: Dokumente, Quittungen und Siegelung

Art. 4 Format der Dokumente

Abs. 1

Diese Bestimmung sieht vor, dass die Behörden, also insbesondere Gerichte, Staatsanwaltschaften und Verwaltungsbehörden auf allen föderalen Stufen und unabhängig davon, ob sie ein Verfahren leiten oder in einer anderen Funktion an einem Verfahren beteiligt sind, ihre Dokumente im Format PDF/A übermitteln. Damit sind die von den Behörden selbst erstellten Dokumente gemeint, wie beispielsweise Urteile, Entscheide, Beschlüsse und Verfügungen oder allfällige Begleitschreiben.

Das archivtaugliche Format PDF/A (in allen Ausprägungen) wird von Behörden verlangt, weil davon auszugehen ist, dass seitens Behörden der Versand und auch die Siegelung ihrer Dokumente (siehe Artikel 22 Absatz 2 BEKJ) automatisiert erfolgt.

Die übrigen Verfahrensbeteiligten (e contrario zu den verfahrensleitenden und verfahrensbeteiligten Behörden) können für ihre Eingaben an Behörden das Format PDF oder PDF/A verwenden. Eine Automatisierung des Prozesses bei den übrigen Verfahrensbeteiligten kann nicht vorausgesetzt werden, da die Benutzung der Plattform für elektronischen Eingaben allen Personen offensteht, also nicht nur den professionellen Benutzerinnen und Benutzern. Für Personen, die selten mit Gerichten und Behörden in Kontakt treten, soll das fehlende PDF/A-Format kein Hindernis sein.

Abs. 2

Die Beilagen können in jeglichem Format übermittelt werden. Immer wenn möglich und sinnvoll sollen jedoch auch Beilagen im Format PDF oder PDF/A übermittelt werden. Die Formate PDF und PDF/A sind die tauglichsten Formate, weil sie in einem hochgradig heterogenen Umfeld mit vielen unterschiedlichen Akteuren (Gerichte,

¹³ SR 172.041.1

Staatsanwaltschaften, Verwaltungsbehörden, Anwaltschaft) maximale Interoperabilität und Reproduzierbarkeit gewährleisten. Grundsätzlich liegt das Risiko, ob eine Behörde eine Beilage öffnen und verwenden kann, bei der Absenderin oder beim Absender. Diese werden sich (beispielsweise aufgrund ihrer anwaltlichen Sorgfaltspflichten) überlegen müssen, ob das empfangende Gericht oder die empfangende Behörde die Beilage öffnen kann. Die Beilagen können direkt an die Plattform übermittelt werden, ohne dass sie vorher noch in ein archivtaugliches Format wie ZIP oder 7-Zip verpackt werden müssen.

Abs. 3

Absatz 3 enthält eine Liste von Formaten, die von den Gerichten und Behörden zwingend geöffnet werden müssen. Damit wird verhindert, dass Gerichte und Behörden gestützt auf Absatz 4 standardmässig die Nachreichung von Beilagen in einem bestimmten Format (z. B. als PDF) fordern können. Diese Liste ist bewusst schlank gehalten und stützt sich auf Formate, die auf allen gängigen Geräten (Windows, macOS, Linux, Tablets, Smartphones) geöffnet werden können. Teilweise gibt es bei einzelnen Formaten weitere Untervarianten, wie dies beispielsweise bei PDF/A der Fall ist. Diese können weiter unterteilt werden in PDF/A-1 bis PDF/A-4. Mit der Nennung von PDF/A sind auch alle Untervarianten in ihren gängigen Ausprägungen eingeschlossen.

Abs. 4 und 5

Die Behörden setzen den Verfahrensbeteiligten eine angemessene Frist an, wenn sie eine Beilage nicht öffnen können. Sie können verlangen, dass die Absenderin oder der Absender die Beilage in einem von der Behörde festgelegten Format einreicht oder der Behörde Zugriff auf die Beilage in geeigneter Weise ermöglicht. Grundsätzlich ist es auch möglich, dass einzelne Gerichte und Behörden (in einem Merkblatt, o. Ä.) festhalten, welche Formate von ihnen verwendet werden können. Der Mindeststandard von Absatz 3 darf dabei jedoch nicht unterschritten werden. Ähnliche Bestimmungen gibt es bereits in der ZPO und StPO (vergleiche Artikel 132 Absatz 2 ZPO und Artikel 110 Absatz 4 StPO).

Der Grund, warum ein Gericht oder eine Behörde die Beilage nicht öffnen kann, ist nicht relevant. Dies kann daran liegen, dass benötigte Software für ein bestimmtes Format nicht installiert ist. Es kann jedoch auch an den eigenen Datensicherheitsbestimmungen liegen, dass Gerichte und Behörden nur spezifische Formate öffnen dürfen. Diese Bestimmung ist aber nicht dahingehend zu verstehen, dass Gerichte und Behörden standardmässig jede Beilage im Format PDF oder PDF/A nachfordern dürfen.

Strukturierte Daten

In der Praxis besteht das Bedürfnis, strukturierte Daten übermitteln zu können. Da für die Übermittlung von Beilagen keine Formate vorgegeben sind, können strukturierte Daten stets als Beilage übermittelt werden.

Aufgrund des Siegelungserfordernisses von Artikel 22 Absatz 2 BEKJ ist es jedoch nicht möglich, dass strukturierte Daten als Dokumente direkt übermittelt werden, da sie nicht gesiegelt werden können. Es ist davon auszugehen, dass die Abläufe für die Übermittlung über eine Plattform besonders bei den Behörden automatisiert erfolgen werden. Die Behörden können in ihrem Prozess automatisch ein Begleitschreiben (im Sinn von Abs. 1) erstellen und siegeln sowie die strukturierten Daten als Beilage übermitteln.

Token

Ein Token oder andere Credentials können als Beilage in einem separaten Dokument übermittelt werden, da es für Beilagen keine Formatvorgaben gibt. Darüber hinaus können Tokens auch in Textform, als QR-Code oder auf andere Weise in den Dokumenten der Behörden oder der übrigen Verfahrensparteien (im Sinn von Abs. 1) übermittelt werden.

Verworfen Variante: Nachfordern des Originalformats

Es wurde geprüft, ob die Behörden aus sachlichen Gründen die Nachreichung des Originalformats verlangen dürfen. Dies wäre beispielsweise denkbar, wenn eine Partei komplexe Tabellenkalkulationen in ein PDF konvertiert und dieses PDF als Beilage einreicht. Aus Sicht der Behörden kann es zu Effizienzsteigerungen führen, wenn sie das Dokument im Originalformat nachfordern können. Dann liegen alle Formeln und Verknüpfungen im Dokument vor, was die Bearbeitung und Nachprüfung erleichtert. Diese Variante wurde aus mehreren Gründen verworfen. Aus Gründen der Rechtssicherheit sollen Parteien Eingaben tätigen und sicher sein können, dass Fristen eingehalten sind, die Eingabe rechtssicher erfolgt ist und auf die Partei kein weiterer Aufwand fällt. Zudem kann das Originalformat Informationen enthalten, die die Partei nicht übermitteln will. Ein Vorteil der Konvertierung in ein Dokument im Format PDF ist, dass nur der aktuelle sichtbare Teil in das PDF-Dokument übertragen wird. Also keine früheren Versionen oder andere Metadaten, die sich bei mehrfacher Bearbeitung angesammelt haben. Zudem können PDF-Dokumente grundsätzlich wieder in die Originalformate zurückkonvertiert werden. Bei reinen Textdokumenten geht das sehr einfach. Im Gegensatz dazu können bei Tabellenkalkulationen nur die Werte, nicht aber die Formeln, zurückübertragen werden.

Verworfen Variante: abschliessende Liste mit zulässigen Formaten

Weiter wurde geprüft, ob für die Beilagen eine abschliessende Liste von zulässigen Formaten vorgegeben werden soll. Es gibt Standardformate, die grundsätzlich auf allen gängigen Geräten (Windows, macOS, Linux, Tablets, Smartphones) geöffnet werden können. Diskussionen im Rahmen der Begleitgruppe haben jedoch gezeigt, dass eine solche Liste nicht zielführend ist. Zudem wäre zu klären, wie mit Formaten umzugehen ist, die nicht auf der Liste sind. Es wäre zu erklären, wieso bestimmte Formate zulässig sind, andere äquivalente Formate hingegen nicht. Zudem müssten besonders nicht-professionellen Benutzerinnen und Benutzer mit erhöhtem Aufwand klären, welche Formate zulässig sind und welche nicht. Das würde die Attraktivität der Plattform für diese Benutzergruppen senken.

Art. 5 Quittungen

Abs. 1

Der Artikel 22 Absatz 4 BEKJ könnte den Eindruck erwecken, dass für jedes übermittelte Dokument eine eigene Quittung erstellt werden muss. Dieser Absatz stellt klar, dass nur eine Quittung erstellt werden muss, auch wenn mehrere Dokumente gleichzeitig übermittelt werden.

Abs. 2

Dieser Absatz regelt, welche Angaben auf den Quittungen mindestens enthalten sein müssen. Diese sind die Art der Quittung, der Name der Absenderin oder des Absenders und der Adressatin oder des Adressaten inklusive der Adresse auf der Plattform. Handelt die Absenderin oder der Absender im Namen einer Organisation, so ist der Organisationsname ebenfalls aufzuführen. Zudem muss auf der Eingangsquittung jedes in der Sendung übermittelte Dokument mit seinem Namen, seiner Grösse und seinem Hashwert aufgeführt werden. Falls aufgrund der Virenprüfung bestimmte Dokumente nicht übermittelt werden, sind darüber hinaus deren Namen und Grössen anzugeben.

Ebenfalls ist der für diese Art der Quittung relevante Zeitpunkt aufzuführen. Der relevante Zeitpunkt stellt auf den tatsächlichen Handlungszeitpunkt ab und nicht auf Beginn oder Ende von gesetzlichen oder prozessualen Fristen. Wird beispielsweise eine Zustellung erstmalig an einem Sonntag abgerufen, so wird dieser Zeitpunkt auf der Quittung festgehalten und ist massgeblich für den Nachweis des Zeitpunkts der Zustellung (vgl. Art. 20 Abs. 2^{ter} f. VwVG i.d.F. des BEKJ und die analogen Parallelbestimmungen). Bei der Nichtabholquittung ist zusätzlich der Zeitpunkt der Übermittlung festzuhalten.

Versendet oder ruft jemand mittels Berechtigungen ab, so ist in der Quittung der Name der Person anzugeben, für die gehandelt wird und nicht der Name der Person, die effektiv die Handlung mittels erteilter Berechtigungen vornimmt.

Bezüglich Grösse und Hashwert: Dies gilt für jedes übermittelte Dokument separat. Es wird also nicht die Gesamtgrösse und der Hashwert der Sendung aufgelistet. Bei übermittelten ZIP-Containern werden die Grösse und der Hashwert der Container selbst, nicht aber der darin enthaltenen Dokumente, auf der Quittung ausgewiesen.

Erkennt die 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, allerdings nur mit Namen und Grösse des Dokuments. Auf den Hashwert kann verzichtet werden, da diese Dokumente nicht übermittelt und somit auch nicht auf Integrität geprüft werden können.

Es ist nicht notwendig, den Namen der Plattform auf der Quittung aufzuführen, da dies aus dem von der Plattform angebrachten Siegel hervorgeht.

Der VE-VEKJ verzichtet darauf, vorzuschreiben, dass die Quittungen auch Angaben enthalten müssen, ob die Übermittlung erfolgreich erfolgt ist oder ob die quittierte Übermittlung verzögert oder abgebrochen wurde. Eine Eingangsquittung wird nach Artikel 22 Absatz 4 Buchstabe a BEKJ erst dann ausgestellt, sobald ein Dokument übermittelt wurde. Vor einer erfolgreichen Übermittlung kann folglich keine Quittung ausgestellt werden.

Abs. 3 bis 5

Die Quittungen sollen einerseits für die Benutzerinnen und Benutzer einfach verständlich, vertrauenswürdig und beweiskräftig sein, um im Rechtsverkehr benutzt werden zu können. Andererseits sollen sie effizient maschinenlesbare Daten bereitstellen können, um automatisiert Einträge in den Systemen der Benutzerinnen und Benutzer vornehmen zu können. Diese beiden Anforderungen lassen sich nur schwerlich in einer einzigen Quittung verwirklichen. Es ist deshalb vorgesehen, dass die Plattformen auch zwei separate Quittungen erstellen können. Erstellt eine Plattform separate Quittungen in für Menschen lesbarer und maschinenlesbarer Form, muss sie nur die menschenlesbare Form im Format PDF/A erstellen und mit einem elektronischen Siegel sowie einem Zeitstempel versehen.

Art. 6 Siegelung der Dokumente durch die übermittelnde Behörde

Gemäss Artikel 22 Absatz 2 BEKJ sind verfahrensleitende und verfahrensbeteiligte Behörden verpflichtet, ihre Mitteilungen zu siegeln und mit einem Zeitstempel zu versehen. Bei Versand durch eine Behörde, muss sie alle Dokumente mit einem Siegel und einem Zeitstempel versehen. Dokumente, die bereits über eine qualifizierte elektronische Signatur oder ein geregeltes elektronisches Siegel zusammen mit einem qualifizierten elektronischen Zeitstempel verfügen, brauchen sie nicht erneut zu siegeln.

Die Plattformen müssen prüfen, ob die Behörden die erforderlichen Siegel und Zeitstempel angebracht haben. Falls ein Siegel oder ein Zeitstempel fehlt, verweigern die Plattformen die Entgegennahme der Dokumente (vgl. Art. 22 Abs. 2 Satz 2 BEKJ).

Art. 7 Siegelung der Dokumente durch die Plattform

Der primäre Zweck der Siegelung ist es, dass die Integrität der gesiegelten Dokumente geschützt respektive überprüfbar gemacht wird. Eine Siegelung verhindert nicht eine Manipulation des gesiegelten Dokuments. Sie ermöglicht jedoch eine Prüfung, ob eine solche Manipulation erfolgt ist.

Generell kann die Siegelung auf mehrere Arten erfolgen. Einerseits kann das Siegel direkt im Dokument selbst angebracht werden. Allerdings unterstützen nicht alle Dateiformate diese Art der Siegelung. Alternativ berechnet das System den Hashwert des zu siegelnden Dokuments und hält ihn in einem anderen, siegelbaren Dokument fest. Mit dem Hashwert in diesem gesiegelten Dokument prüft die zuständige Person, ob das zu siegelnde Dokument geändert worden ist. Beide Verfahren führen zum gleichen Ergebnis.

Zudem besteht Seitens der Anwaltschaft das Bedürfnis, dass die übermittelten Dokumente von den Plattformen nicht geändert werden. Es bestehen Bedenken, dass die Behörden und andere verfahrensbeteiligte Personen nicht mehr nachvollziehen können, welche Version des Dokuments innerhalb der Frist eingereicht worden ist. Wird das Siegel direkt in den übermittelten Dokumenten angebracht, verändert dies die Dokumente. Wird das Siegel in einem separaten Dokument angebracht, verbleiben die übermittelten Dokumente unverändert.

Abs. 1

Die vorliegende Bestimmung regelt die Siegelung für den Fall, dass mehrere Dokumente zusammen übermittelt werden. Dies dürfte dem Regelfall entsprechen, da eine Eingabe häufig aus einer Rechtsschrift und Beilagen besteht. In diesem Fall bringt die Plattform das Siegel und den Zeitstempel in einem separaten Dokument an. So kann den oben genannten Bedenken und dem Umstand, dass die Beilagen nach Artikel 4 Absatz 2 in jedem beliebigen Format übermittelt werden können, Rechnung getragen werden.

Abs. 2

Wenn ein Dokument bereits gesiegelt ist, dann trägt eine weitere Siegelung nichts zur Belegung der «Unverändertheit» bei. Deshalb ist es nicht erforderlich, bei bereits vorhandenem Siegel erneut zu siegeln.

Akteneinsicht

Artikel 6 und 7 VE-VEKJ gelten nicht für die Akteneinsicht, da bei dieser kein Siegel anzubringen ist (Art. 22 BEKJ e contrario). Die Siegelungspflicht (Art. 22 Abs. 2 und 3 BEKJ) soll nur für Zustellungen und Eingaben (vgl. beispielsweise Art. 130 ff. und Art. 136 ff. ZPO) gelten. Mit diesen Prozessschritten können den an einem Verfahren beteiligten Parteien Fristen angesetzt werden bzw. können letztere neue Dokumente in ein Verfahren einbringen. Aus diesem Grund ist es notwendig, mit einem Siegel die Integrität der eingereichten Dokumente bzw. mit einem Zeitstempel die Einhaltung einer Frist sicherzustellen.

Der Gesetzgeber wollte nie eine Siegelungspflicht für die Akteneinsicht einführen. Bei der Akteneinsicht werden keine neuen Dokumente in ein Verfahren eingebracht, sondern es wird einer Partei lediglich ermöglicht, die bereits vorhandenen Dokumente einzusehen. Folglich ist auch keine Siegelung nötig. Ein Zeitstempel ist ebenfalls unnötig, da die Behörde bei der Gewährung der Akteneinsicht nur festlegt, wie lange der Zugriff auf die Akten gewährt wird. Wann die Partei während des festgelegten Zeitraums Einsicht in die Akten nimmt, spielt keine Rolle.

4. Abschnitt: Authentifizierung, Profile, Schnittstellen und Berechtigungen

Art. 8 Authentifizierung der Benutzerinnen und Benutzer

Abs. 1

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 AGOV einerseits native elektronische Identitäten bietet, die im Endbenutzenden-Self-Service in AGOV registriert werden. Zudem kann AGOV auch weitere anerkannte elektronische Identitäten fördern und als autonome Credentials für Login-Vorgänge benutzen.¹⁴ Da AGOV eigene elektronische Identitäten aufgrund einer Prüfung erstellen oder bestehende anerkannte Identitäten fördern kann, erfüllt AGOV die Voraussetzungen nach Artikel 20 Absatz 2 BEKJ.

Die Vorteile von AGOV sind insbesondere, dass jede Person mit einem gültigen Reisepass oder einer gültigen Identitätskarte ein AGOV-Login auf Stufe 300 erhalten kann (sogenannte Universalität). Somit können auch Personen im Ausland ohne schweizerischen Pass oder schweizerische Identitätskarte am elektronischen Rechtsverkehr in der Schweiz teilnehmen. Dies betrifft insbesondere Anwältinnen und Anwälte aus der EU, die auch vor schweizerischen Gerichten Parteien vertreten dürfen. Für diese entfällt bei Nutzung der elektronischen Kommunikation über die Plattform die Bezeichnung eines schweizerischen Zustellungsdomizils (beispielsweise Art. 11b Abs. 1 VwVG und Art. 39 Abs. 3 des Bundesgerichtsgesetzes vom 17. Juni 2005 [BGG]¹⁵ in der Fassung des BEKJ).

Wer über einen schweizerischen elektronischen Identitätsnachweis für natürliche Personen (E-ID) verfügt, kann ohne weiteren Nachweis ein AGOV-Login auf Stufe 300 einrichten. Zudem muss auch die schweizerische E-ID als Identitätsnachweis aufgrund von Artikel 24 Bundesgesetz vom 20. Dezember 2024 über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz; BGEID¹⁶) akzeptiert werden. Eine ausdrückliche Nennung der schweizerischen E-ID ist deshalb nicht notwendig.

Es könnten zwar noch weitere elektronische Identitätsnachweise zugelassen werden, doch diese müssten von der zentralen Plattform und allenfalls weiteren Plattformen

¹⁴ Vgl. Informationen für Behörden, abrufbar unter www.agov.admin.ch > Für Behörden

¹⁵ SR 173.110

¹⁶ BBl 2025 20

auch integriert werden. Dies würde jedoch die Komplexität erhöhen und weitere Kosten verursachen. Da grundsätzlich jede Person ein AGOV-Login auf Stufe 300 erhalten kann, sind weitere Identitätsnachweise nicht notwendig.

Abs. 2

Setzen die Kantone weitere Plattformen im Sinn von Artikel 4 BEKJ ein, müssen sie ebenfalls AGOV als Authentifizierungsdienst verwenden. Sie können jedoch zusätzlich andere Authentifizierungsdienste einsetzen, sofern diese eine vergleichbare Authentifizierungsqualität bieten. Zudem müssen die Kantone die schweizerische E-ID gemäss BGEID als Identitätsnachweis akzeptieren.

Abs. 3

Gemäss Artikel 21 BEKJ müssen sich Benutzerinnen und Benutzer, die eine Plattform über die Anwendung einer Behörde nutzen, gegenüber der Plattform nicht authentifizieren, wenn die Betreiberin der Plattform dies bewilligt. Es wird einige Zeit dauern, bis alle interessierten Behörden ihre Anwendungen über eine Schnittstelle mit der Plattform verbunden haben. Zudem ist denkbar, dass kleine Behörden, die nur sporadisch über die Plattform kommunizieren, weiterhin das Web-Login der Plattform benutzen werden. In diesen Fällen ist es sinnvoll, dass die Betreiberinnen von Plattformen auch weitere Identitätsanbieter (z. B. kantonseigene IDP) akzeptieren können, soweit diese ebenfalls ein angemessenes Schutzniveau bieten. Eine Pflicht diese weiteren IDPs zu akzeptieren, besteht seitens der Betreiberinnen nicht.

Art. 9 Profile

Abs. 1

Die Plattformen müssen es ermöglichen, dass ein Benutzerkonto mehrere Profile haben kann. Dadurch können die Benutzerinnen und Benutzer der Plattformen mit nur einem Konto in verschiedenen Rollen kommunizieren. So kann eine natürliche Person als Anwältin oder als Anwalt dem Obligatorium unterstehen. Diese Person möchte die Plattform auch privat nutzen – also ausserhalb des Obligatoriums. Zudem ist diese Person noch Verwaltungsrätin oder Verwaltungsrat in einer oder mehreren Aktiengesellschaften und auch Vorstandsmitglied eines örtlichen Vereins. Mit den unterschiedlichen Profilen kann diese Person jeweils in die entsprechende Rolle schlüpfen und Sendungen versenden und empfangen.

Abs. 2 bis 4

Um Falschzustellungen möglichst zu vermeiden, müssen die einzelnen Profile mit gewissen Mindestangaben versehen werden.

Bei Behörden gehört zu den verlangten Mindestangaben: der Name der Behörde, deren Postadresse sowie die Bezeichnung ihres Siegels. Während der Name der Behörde und deren Postadresse dazu dienen, die richtige Behörde zu finden, dient die

Angabe des Siegelnamens einem anderen Zweck. Wenn Behörden Zustellungen tätigen, sind sie verpflichtet, ihre Mitteilung mit einem elektronischen Siegel zu versehen. Mit der Hinterlegung der Bezeichnung ihres Siegels im Profil können die Plattformen prüfen, ob mindestens ein Dokument mit dem korrekten Siegel versehen ist (vgl. Art. 22 Abs. 2 BEKJ).

Als Bezeichnung des Siegels dient das «Common Name» (CN) Feld in den Zertifikaten. Der CN ist ein entscheidender Bestandteil von X.509-Zertifikaten und dient als primäre Kennung für den Zertifikatsinhaber. Sein Zweck und seine Verwendung variieren je nach Zertifikatstyp. Bei SSL/TLS Zertifikate muss der CN genau mit dem Domainnamen der Webseite übereinstimmen. In Bezug auf Siegelung von Dokumenten enthält der CN den Namen der Organisation.

Natürliche Personen müssen Vornamen, Namen, Postadresse und Geburtsdatum angeben. Bei Organisationen ist der Name oder die Firma sowie die Postadresse anzugeben. Mit diesen Angaben kann eine Falschzustellung faktisch ausgeschlossen werden.

Legt eine Person ein Profil an, mit welchem sie in der Funktion handelt, die dem Obligatorium untersteht, dann gibt sie ihre allfällige Organisationszugehörigkeit und geschäftliche Postadresse an. In der Anwaltschaft ist es üblich, dass auch der Name der Anwaltskanzlei gegen aussen getragen wird – insbesondere bei Schreiben wird oft das «Kanzleipapier» verwendet.

Organisationen im Sinne von Absatz 3 und 4 können juristische Personen sein, aber auch andere Organisationsformen wie einfache oder kollektive Gesellschaften. Besonders Anwaltskanzleien sind oft als einfache oder kollektive Gesellschaften ausgestaltet.

Gehört das Profil einer natürlichen Person, so ist aufgrund von AGOV die Identität dieser Person bestätigt. Bei Organisationen gibt es keinen solchen Prozess – der Name der Organisation und die Vertretungsberechtigung wird nicht geprüft, allerdings ist bei einer Organisation immer eine verantwortliche Person eingetragen. Beim Erstellen solch eines Organisationsprofils ist es die natürliche Person, der das Konto gehört. Dies kann nachträglich geändert werden, wobei auch die Einwilligung der neuen verantwortlichen Person notwendig ist. Die Behörden werden zukünftig, wie bereits auch heute, im Rahmen der Verfahren zu prüfen haben, ob die entsprechende Organisation besteht und ob die Vertretungsvollmacht gegeben ist.

Art. 10 Schnittstelle

Der Zugang über die Schnittstelle erfolgt über ein API-Token – einem sicheren, alphanumerischen Schlüssel. Das API-Token funktioniert wie ein digitales Passwort, das speziell für maschinelle Kommunikation zwischen Anwendungen oder Diensten generiert wird, ohne dass sensible Benutzerdaten geteilt werden müssen. Solche Tokens werden häufig eingesetzt, um sichere und kontrollierte Zugriffe zu ermöglichen.

Wenn solche Tokens eingerichtet werden, gleicht dies der Vergabe von Berechtigungen an eine andere Benutzerin oder an einen anderen Benutzer. Deshalb müssen die API-Tokens regelmässig bestätigt werden, ansonsten werden sie automatisch gelöscht oder gesperrt.

Art. 11 Bestätigung und Entzug der Berechtigungen

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). Dies kann weitreichende Folgen haben. Deshalb sollen die Benutzerinnen und die Benutzer die Berechtigungen mindestens einmal pro Jahr prüfen.

Falls die Person die Berechtigungen weder bestätigt noch ablehnt, also nicht reagiert, dann entziehen die Plattformen die Berechtigungen automatisch drei Monate nach der letzten Bestätigungsaufforderung.

Die betroffenen Benutzerinnen und Benutzer werden über den automatischen Entzug benachrichtigt. Dies umfasst die Benutzerinnen und Benutzer, die Berechtigungen erteilt oder erhalten haben. Sollte der Entzug der Berechtigungen nicht erwünscht sein, können die Betroffenen entsprechende Schritte einleiten, um die Berechtigungen erneut zu erteilen. Beispielsweise kann die berechtigte Person Kontakt mit der berechtigungserteilenden Person aufnehmen und auf diesen Umstand hinweisen.

5. Abschnitt: Datenschutz, Datensicherheit und Virenprüfung

Art. 12 Maximale Aufbewahrungsfrist für Dokumente und Quittungen

Abs. 1

Artikel 22 Absatz 5 BEKJ enthält eine Mindestfrist von 90 Tagen, während dessen die Plattformen die übermittelten Dokumente und erstellten Quittungen nicht automatisch vernichten dürfen. Mit der vorliegenden Bestimmung wird die maximale Aufbewahrungsfrist auf sechs Monate festgelegt. Die Aufbewahrungsfristen nach Artikel 21 der Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)¹⁷ bleiben vorbehalten.

Die Vernichtung muss nicht exakt zum Ablauf von sechs Monate nach der Übermittlung erfolgen. Die Plattformen können, je nach Auslastung, noch mehrere Stunden zuwarten. Jedoch muss die Vernichtung innert 24 Stunden nach Ablauf der sechs Monate erfolgen.

¹⁷ SR 780.11

Abs. 2

Bei Akten, die im Rahmen der Akteneinsicht zur Verfügung gestellt werden, wird zum Zeitpunkt der Bereitstellung angegeben, bis wann die Akten verfügbar bleiben. Nach diesem Zeitpunkt vernichten die Plattformen die Akten automatisch. Die Frist von sechs Monaten nach Absatz 1 gilt somit nicht.

Verworfenen Variante

Es wurde ebenfalls in Betracht gezogen, die maximale Aufbewahrungsfrist an die Inaktivität in einem Verfahren festzulegen. Wenn also über einen bestimmten Zeitraum in einem Verfahren keine neuen Zustellungen oder ähnliches erfolgen, werden die Dokumente gelöscht. Diese Variante wurde verworfen, weil die Plattformen aus technischen Gründen nicht immer erkennen können, ob eine Zustellung zu einem bestehenden oder einem neuen Verfahren gehört.

Art. 13 *Datensicherheit*

Der Missbrauch von Informationen und die Störung von Informationssystemen können wesentliche Interessen der Schweiz und die Rechte von Personen schwerwiegend beeinträchtigen. Mit der Entwicklung zu einer Informationsgesellschaft sind die entsprechenden Bedrohungen komplexer und dynamischer geworden. Mit dem Informationssicherheitsgesetz vom 18. Dezember 2020 (ISG)¹⁸ hat das Parlament einen einheitlichen gesetzlichen Rahmen für die Steuerung und Umsetzung der Informationssicherheit im Zuständigkeitsbereich des Bundes geschaffen, basierend auf internationalen Standards.

Da der Bund sowohl an der zentralen Plattform wie auch an der allgemeinen Plattform für Verwaltungsverfahren beteiligt ist, liegt es nahe, die Anforderungen an die Datensicherheit nach dem Informationssicherheitsgesetz zu regeln. Mit dem ISG hat der Bund die wichtigsten Rechtsgrundlagen für die Sicherheit von Informationen und Informatikmitteln des Bundes in einem einzigen Erlass zusammengefasst. Damit soll ein möglichst einheitliches Sicherheitsniveau erreicht werden, das auch für die Plattformen nach dem BEKJ gelten soll. Die vorliegende Bestimmung ist nur für die Kantone von Bedeutung, da für den Bund die Vorgaben nach dem ISG ohnehin anwendbar sind.

Zudem übt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) die datenschutzrechtliche Aufsicht über die Plattform aus (Art. 27 Abs. 6 BEKJ), weswegen auch Artikel 8 DSG zur Anwendung gelangt.

¹⁸ SR 128

Art. 14 Virenprüfung

Abs. 1

Aufgrund der Vorgaben zum Datenschutz und der Datensicherheit (Art. 27 f. BEKJ) müssen die Plattformen übermittelte Dokumente auf Schadsoftware prüfen. Aus sprachlichen Gründen verwendet der VE-VEKJ die Begriffe «Virenprüfung» und «Virus». Mit diesen Begriffen ist Schadsoftware und Prüfung auf Schadsoftware im Allgemeinen gemeint. Je grösser die übermittelten Dokumente sind, umso mehr Ressourcen nimmt eine Antivirenprüfung in Anspruch. Die Plattformen können übermittelte Dokumente bis zu einer Grösse von 64 Megabyte ohne Einbusse an der Leistungsfähigkeit prüfen. Daher wird diese Grösse als Grenzwert für eine ordentliche Virenprüfung eingeführt.

Abs. 2

Werden Dokumente übermittelt, die grösser als 64 Megabyte sind, können die Plattformen diese Dokumente in 64-Megabyte-grosse-Teile aufspalten und diese Teile einer Virenprüfung unterziehen. Das Problem dabei: Schadsoftware kann innerhalb eines Dokuments verteilt sein. Durch das Aufspalten kann die Schadsoftware möglicherweise nicht korrekt erkannt werden. Daher sieht der VE-VEKJ vor, dass die Plattformen diese Dokumente speziell markieren. Die Empfängerinnen und Empfänger können dadurch die notwendige Sorgfalt im Umgang mit diesen Dokumenten walten lassen.

Abs. 3

Es können bewusst auch Dokumente übermittelt werden, die Schadsoftware enthalten, beispielsweise wenn Strafverfolgungsbehörden Computer oder Mobilgeräte als Beweismittel sicherstellen. Die in diesen Geräten enthaltene Schadsoftware ist dann Teil der Beweismittel und muss unverändert bleiben. Der VE-VEKJ sieht deswegen vor, dass die Betreiberin einer Plattform auf Ersuchen auf die Virenprüfung verzichten kann.

Der Verzicht kann mündlich oder schriftlich erfolgen. Er kann unter Vorbehalt von Haftungsausschlüssen usw. erteilt werden. Er kann einmalig, für eine bestimmte Zeitdauer oder eine unbestimmte Zeitdauer erteilt werden. In der Regel erfolgt die Einwilligung schriftlich, kann aber in dringenden Fällen vorab mündlich erteilt werden.

Abs. 4

Findet keine Virenprüfung oder eine eingeschränkte nach Absatz 2 statt, dann sind diese Dokumente durch die Plattform speziell zu kennzeichnen. Die Empfängerinnen und Empfänger können dadurch die notwendige Sorgfalt im Umgang mit diesen Dokumenten walten lassen.

Abs. 5

Stellt die Plattform fest, dass ein oder mehrere übermittelte Dokumente Schadsoftware enthalten, so verweigert die Plattform die Übermittlung dieser Dokumente an die Empfängerinnen und Empfänger. Die restlichen (nicht betroffenen) Dokumente, die gleichzeitig übermittelt werden sollen, werden an die Empfängerinnen oder die Empfänger übermittelt. Zu Beweis Zwecken enthält die Quittung nach Artikel 11 eine Liste der wegen Schadsoftware nicht übermittelten Dokumente und deren Grösse. Das geltende Prozessrecht regelt zudem bereits, wie mit solchen mangelbehafteten Eingaben umzugehen ist (vgl. bspw. Art. 132 Abs. 1 ZPO). Üblicherweise wird in solchen Fällen eine angemessene Nachfrist zur Übermittlung der fehlenden Dokumente gewährt.

In der Praxis sollte diese Norm nur selten zur Anwendung kommen, da ein grosser Teil der Dokumente im PDF- oder PDF/A-Format übermittelt werden wird. Werden neue PDF-Dokumente unter Verwendung von legitimen Konvertierungstools wie die «Speichern unter»- oder «Exportieren»-Funktion von Microsoft Office oder das Drucken in eine PDF-Datei beispielsweise mittels PDF24 erstellt, dann rendert der Konvertierungsprozess den sichtbaren Inhalt des Dokuments im Wesentlichen in ein statisches Format und entfernt dabei ausführbare Elemente, die Schadsoftware enthalten könnten. Es ist zwar nicht undenkbar, dass sich Schadsoftware so tief in das Betriebssystem, PDF-Druckertreiber oder ähnliches einnistet und dann Schadsoftware in die neu erstellten PDF-Dokumente während des Konvertierungsprozesses einspeist. Es gibt jedoch keinen bekannten Fall einer solchen Schadsoftware.

6. Abschnitt: Gebühr für die Nutzung der zentralen Plattform

Gemäss Artikel 32 BEKJ erhebt die öffentlich-rechtliche Körperschaft jährlich von den Behörden Gebühren für die Benutzung der Plattform. Dabei kann der Bundesrat Pauschalen vorsehen. Die Botschaft führt in den Erläuterungen zu Artikel 32 BEKJ aus, dass sich Begriff Pauschale nicht nur auf die Gebühren selbst, sondern auch auf die Rechnungstellung bezieht. So kann der Bundesrat zur Vereinfachung der Abrechnung vorsehen, dass die Gebühren von den Kantonen und dem Bund zusammengefasst erhoben werden können, statt von jeder einzelnen Behörde.

Art. 15 Berechnung der Gebühr

Abs. 1

Die Bestimmung legt die Bemessungsgrundlage der jährlichen Gesamtgebühr fest. Die Gebühr ist so auszugestalten, dass sie die Kosten für Betrieb und Weiterentwicklung der zentralen Plattform deckt (Kostendeckungsprinzip). Zusätzlich ist eine Liquiditätsreserve zulässig, begrenzt auf 10 % der jährlichen Betriebskosten. Die Reserve dient ausdrücklich der Sicherstellung der Liquidität der öffentlich-rechtlichen Körperschaft (z. B. zur Überbrückung von Zahlungsflüssen, unerwarteten Aufwänden, kurzfristigen Finanzierungsspitzen). Es handelt sich um einen beschränkten Puffer, nicht um eine Gewinnmarge. Einnahmen aus Leistungsbezügen nichtmitgliederschaftlicher Kantone sind bei der Berechnung der Gesamtgebühr in Abzug zu bringen. Damit wird

verhindert, dass Mitglieder Kosten tragen, die bereits durch Dritte (Nichtmitglieder) gedeckt sind, und es wird eine Doppelbelastung vermieden.

Abs. 2

Das EJPD legt die jährliche Gebühr gestützt auf die Finanzplanung der öffentlich-rechtlichen Körperschaft alle drei Jahre fest. Grundsätzlich erfolgt keine jährliche Gebührenanpassung. Dies schafft Planbarkeit und reduziert den administrativen Aufwand (Tarif-/Gebührenanpassungen nicht jährlich), ohne die Kostendeckung aus dem Blick zu verlieren.

Die Festsetzung orientiert sich an nachvollziehbaren Planungsparametern (Budget/Mehrjahresplanung, Investitions- und Entwicklungsroadmap, Betriebskalkulation). Diese Planungsparameter wirken als Sachlichkeits- und Dokumentationsanforderungen an den Gebührenentscheid des EJPD. In der Praxis bedeutet dies, dass die öffentlich-rechtliche Körperschaft dem EJPD jährlich aktualisierte Dokumentationen zu liefern hat. Alle drei Jahre legt das EJPD die Gebühren formell durch Entscheid fest.

Abs. 3

Falls das EJPD im Sinn von Absatz 2 feststellt, dass die Gebühr die Kosten für Betrieb und Weiterentwicklung nicht deckt oder, dass die Reserve die Limite nach Absatz 1 überschreitet, kann es die Gebühr anpassen. Dieser Absatz wirkt als Korrektiv zum Dreijahresrhythmus: Wenn sich Prognosen als falsch erweisen oder Kosten unerwartet steigen und die Reserve nicht ausreicht, soll die Finanzierung sichergestellt bleiben. Das Gleiche gilt für den Fall, dass die Gebühren zu hoch angesetzt und die Reserven entsprechend zu hoch geworden sind.

Verworfenne Variante: Aufbaukosten

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 Artikel 33 BEKJ ein.

Art. 16 Aufteilung der Gebühr

Bei der Pauschalerhebung der Gebühren stellt sich die Frage, welchen Anteil der Bund und welche Anteile die Kantone tragen sollen. In der Botschaft¹⁹ zum BEKJ wurden die vom Bundesgericht für das Jahr 2020 erhobenen Statistiken aufgeführt. Unter

¹⁹ BBl 2023 679, S. 37 f.

Berücksichtigung der durch die Bundesanwaltschaft und kantonalen Staatsanwaltschaften abgeschlossenen Verfahren lag der Anteil des Bundes bei rund 2.17 %. Zwischenzeitlich hat das Bundesgericht die Statistiken für das Jahr 2024 aktualisiert:

Abgeschlossene Verfahren	Bund	Kantone	Total
durch Gerichtsbehörden	15 090	390 899	405 989
durch Bundes-/Staatsanwaltschaft	1 646	550 458	552 104
Total	16 736	941 357	958 093
Verhältnis	1.75 %	98.25 %	100 %

Gegenüber dem Jahr 2020 ist die Zahl der erledigten Verfahren des Bundes leicht geschrumpft. Allerdings sind in diesen Statistiken die Verwaltungsstrafverfahren des Bundes und der Kantone nicht eingeschlossen. Deren Zahl lässt sich ohne erheblichen Aufwand nicht eruieren. Vor allem im Bereich der eidgenössischen Steuern, insbesondere der Mehrwertsteuer, beim Zoll und bei der Eidgenössischen Spielbankkommission dürfte eine nicht unerhebliche Anzahl Verwaltungsstrafverfahren dazukommen.

Aus folgenden Gründen ist es jedoch angemessen, den Pauschalanteil für den Bund deutlich höher, nämlich auf 10 %, anzusetzen: Einerseits tätigen die kantonalen Gerichte gewisse Vorarbeiten für das Bundesgericht, wie das Digitalisieren von papierernen Eingaben und Beilagen. Andererseits führt die Digitalisierung der Justiz auch zu einem Effizienzgewinn beim Bund, welcher nicht in Zahlen ausgedrückt werden kann. Die höhere Ansetzung trägt auch dem Umstand Rechnung, dass dem Bund in institutioneller Hinsicht in der Körperschaft von Gesetzes wegen ein erhebliches Gewicht zukommt. Die Vereinbarung zur öffentlich-rechtlichen Körperschaft sieht ihrerseits vor, dass der Bund im Vorstand, dem obersten strategischen Gremium der Körperschaft, mit zwei von sieben Mitgliedern vertreten ist.

Das Projekt Justitia 4.0 geht aktuell von jährlichen Kosten für den Betrieb und die Weiterentwicklung der zentralen Plattform in Höhe von 10 bis 12 Millionen Franken pro Jahr aus. Bei einer 10 % Beteiligung des Bundes macht dies 1 000 000 bis 1 200 000 Franken seitens des Bundes und 9 000 000 bis 10 800 000 Franken seitens der Kantone aus.

Der Anteil des Bundes wird je zur Hälfte von der Bundesverwaltung und von den eidgenössischen Gerichten getragen. Der Anteil der Kantone wird auf die einzelnen Kantone gemessen an ihrem Bevölkerungsanteil aufgeteilt.

Allgemeine Gebührenverordnung

Soweit der VE-VEKJ keine besonderen Regelungen trifft, gilt die AllGebV.

Verworfenene Variante: Effektive Nutzung

Statt Pauschalanteilen aufgrund der Bevölkerungsanzahl und der erledigten Verfahren für den Bund könnten die Gebühren auch auf der Grundlage der effektiven Nutzung der zentralen Plattform erhoben werden. Die zentrale Plattform erhebt bereits Statistiken bezüglich der Nutzung und kann für die Gebührenrechnung detaillierte Nutzungsstatistiken der einzelnen Behörden zur Verfügung stellen.

Das Problem bei der Gebührenerhebung nach der effektiven Nutzung liegt darin, dass ohne schweizweites Obligatorium die Nutzung sehr unterschiedlich ausfallen kann. So würden Kantone – oder Bund – einen deutlich grösseren Anteil der Kosten tragen, wenn diese Kantone oder der Bund das Obligatorium vorzeitig einführen. Kantone, die erst später das Obligatorium einführen, würden gleichzeitig profitieren.

Art. 17 Gebührenanteil der Bundesverwaltung und der Bundesanwaltschaft

Abs. 1

Das EJPD bezahlt die von der Bundesverwaltung geschuldete Gebühr. Es fungiert als zentrale Zahlstelle gegenüber der öffentlich-rechtlichen Körperschaft. Dies vereinfacht die Abrechnung. Es geht dabei um die Zahlungsabwicklung und die Zuständigkeit nach aussen, nicht um die interne Kostenverteilung.

Abs. 2

Der Bundesrat legt die interne Aufteilung des Bundesverwaltungsanteils auf die Departemente, die Bundeskanzlei und die Bundesanwaltschaft jeweils für drei Jahre fest. Damit erfolgt ein einheitlicher und politisch legitimer Umlageentscheid für die Bundesverwaltung. Aufgrund der mehrjährigen Gebührenfestsetzung ergibt sich auch Sicherheit in der Planung.

Abs. 3

Die Departemente und die Bundeskanzlei können ihren Anteil an den ihnen unterstellten zentrale und dezentrale Verwaltungseinheiten weiterverrechnen. Damit können die Departemente auf ihrer Stufe dem Verursacherprinzip Rechnung tragen. Es handelt sich hierbei um eine Kann-Bestimmung; die Departemente und die Bundeskanzlei sind nicht zur Kostenumlage verpflichtet.

Da die Bundesanwaltschaft über keine ihr unterstellten Verwaltungseinheiten verfügt, erübrigt sich eine Kostenumlage bei ihr.

Art. 18 Gebührenanteil der eidgenössischen Gerichte

Abs. 1

Das Bundesgericht bezahlt als Kostenstelle den Anteil der eidgenössischen Gerichte. Dadurch zentralisiert das Bundesgericht, gleich wie bei der Bundesverwaltung, die

Zahlung nach aussen für die gesamte Gerichtsbarkeit des Bundes. Dies vereinfacht die Abrechnung und Zahlungsabwicklung.

Abs. 2

Das Bundesgericht legt den Verteilungsschlüssel für die eidgenössischen Gerichte fest. Vor der Festlegung hört das Bundesgericht die anderen eidgenössischen Gerichte an, um Fairness und Akzeptanz zu gewährleisten. Dies entspricht zudem dem aktuellen Recht: Gemäss Artikel 1 Absatz 2 BGG übt das Bundesgericht die Aufsicht über die Geschäftsführung des Bundesstrafgerichts, des Bundesverwaltungsgerichts und des Bundespatentgerichts aus. Als Aufsichtsinstrumente stehen dem Bundesgericht unter anderem die Finanzaufsicht zur Verfügung, welche durch eine mehrjährige gemeinsame Finanzplanung sowie Prüfung und Besprechung der Entwürfe des Voranschlags und der Jahresrechnung erfolgt (Artikel 3 Buchstabe c i. V. m. Artikel 6 Buchstabe a und b des Aufsichtsreglements des Bundesgerichts vom 11. September 2006²⁰).

Im Gegensatz zur Bundesverwaltung gibt es keinen expliziten Zyklus für die Festlegung der Aufteilung. Die Aufteilung kann also flexibler angepasst werden. Zum Beispiel kann die Festlegung des Verteilungsschlüssels jährlich oder bei stark veränderter Nutzung erfolgen.

Art. 19 Fälligkeit

Abs. 1

Die öffentlich-rechtliche Körperschaft erhebt die Gebühren jährlich. Sie werden jeweils am 1. Januar fällig. Damit wird sichergestellt, dass die öffentlich-rechtliche Körperschaft über genügend Liquidität verfügt.

Abs. 2

Diese Bestimmung enthält eine Sonderregel für das erste Betriebsjahr. Für das erste Betriebsjahr wird die Gebühr an dem Tag fällig, an dem die Verordnung in Kraft tritt. Dadurch lässt sich eine Finanzierungslücke vermeiden, falls der Regelstichtag (1. Januar) nicht mit dem Inkrafttretensdatum zusammenfällt.

Art. 20 Rechnungsstelle der Kantone

Jeder Kanton benennt eine einzige Rechnungsstelle, um die Rechnungsstellung und den Zahlungsverkehr mit der öffentlich-rechtlichen Körperschaft zu vereinfachen.

²⁰ SR 173.110.132.

Art. 21 Evaluation der Gebührenregelung

Aufgrund des grossen Spielraums, den der Gesetzgeber dem Bundesrat bei der Festlegung der Höhe zugestanden hat, ist es angezeigt, die vorliegende Regelung nach einer gewissen Zeit zu überprüfen. Dabei ist zu prüfen, ob die Regelung im Vollbetrieb noch sachgerecht, finanzierungsstabil und systematisch stimmig ist. Das EJPD wird beauftragt, die Evaluation zwei Jahre, nachdem die Nutzung der zentralen Plattform im Bund und in allen Kantonen in den vom BEKJ erfassten Verfahren obligatorisch geworden ist, durchzuführen. Damit stellt das EJPD sicher, dass die Evaluation auf Realbetriebsdaten basiert. In die Evaluation ist auch der Preisüberwacher miteinzubeziehen.

2. Kapitel: Digitalisierung von physischen Dokumenten

Art. 22

Die gesetzlichen Grundlagen zur Digitalisierung von physischen Dokumenten ergeben sich aus den jeweiligen Prozessgesetzen in Verbindung mit Artikel 29 BEKJ. In Bezug auf das Bundesverwaltungsgericht ergibt sich die gesetzliche Grundlage nicht direkt aus dem VwVG, sondern aus Artikel 37a des Verwaltungsgerichtsgesetzes vom 17. Juni 2005²¹.

Abs. 1 und 2

Die physisch eingegangenen Dokumente sind von den Gerichten und Behörden in das Format PDF/A zu digitalisieren. Zusätzlich sind die digitalisierten Dokumente mit einer Texterkennung (Optical Character Recognition [OCR]) zu versehen. Die OCR macht den Text durchsuchbar und bearbeitbar, indem es handschriftliche oder gedruckte Buchstaben in maschinenlesbare Daten umwandelt. Die Texterkennung dient der Effizienz: Digitale Dokumente können leichter gespeichert, durchsucht und weiterverarbeitet werden. Dabei ist nicht verlangt, dass die Durchsuchbarkeit mittels Texterkennung zu 100 % akkurat ist, sondern es soll nach «Best Effort» automatisiert erfolgen. Beispielsweise wird die Texterkennung bei eigenhändig geschriebenen Texten (beispielsweise ein Testament), je nach Handschrift, nicht sehr akkurat sein.

Die nach diesem Artikel elektronisch erstellten Dokumente gelten als massgebliche Version (vgl. Art. 29 Abs. 3 BEKJ).

Die digitalisierten Dokumente müssen mindestens eine Farbtiefe von 8 Bit (für 256 Farb- oder Grauabstufungen) und eine Auflösung von 300 DPI aufweisen, um Klarheit und Lesbarkeit zu gewährleisten. Bei Bedarf – zum Beispiel bei farbigen oder detail-

²¹ SR 173.32

lierten Originalen – sind höhere Werte (z. B. 24 Bit Farbtiefe oder 600 DPI) vorzusehen. Damit standardisiert der Bundesrat die Mindestqualität und stellt sicher, dass Dokumente auch bei Vergrösserung oder Druck scharf bleiben.

Abs. 3

Die Behörden müssen eine angemessene Qualitätskontrolle durchführen, um zu gewährleisten, dass die digitalisierten Dokumente dem Original entsprechen – sowohl visuell (z. B. Layout, Bilder) als auch inhaltlich (z. B. Textgenauigkeit). Dies umfasst die Vermeidung von Fehlern, wie fehlende Seiten, unklare oder unleserliche Stellen sowie verzerrte Abbildungen. Die digitale Version muss als vollwertiger Ersatz für das Original dienen. In der Praxis bedeutet das die Einführung von Prozessen wie stichprobenartiger manueller Überprüfung, automatisierter Validierung oder Zertifizierung. Das genaue Verfahren zur Qualitätskontrolle wird den Behörden überlassen.

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

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

Art. 23 Eignungsvoraussetzungen

Die Aktenweitergabe darf nach den einschlägigen Prozessgesetzen auch über andere Wege als über die gemäss BEKJ vorgesehenen Plattformen erfolgen. Dabei müssen aber folgende Anforderungen sichergestellt sein:

Bst. a

Die Zeitpunkte der Übermittlung müssen in geeigneter Weise aufgezeichnet werden. Der VE-VEKJ überlässt es dem technischen System, wie die Zeitpunkte genau festgehalten werden. Dies kann mittels separater Quittungen, die ausgestellt werden oder einer Protokolldatei oder einem Audit Trail erfolgen. Wichtig ist jedoch, dass die Zeitpunkte (nachträglich) nicht manipuliert werden können, ohne dass dies erkennbar ist.

Bst. b

Zusätzlich zur Aufzeichnung der Zeitpunkte muss auch sichergestellt werden, dass die Zeitpunkte mit der offiziellen Schweizer Zeit übereinstimmen. Geringfügige Abweichungen bis zu einer Minute von der offiziellen Schweizer Zeit sind zulässig. Auch wenn eine Minute als lang erscheinen mag: Eine unerwartet hohe Systembelastung kann solchen Verzögerungen verursachen.

Bst. c

Diese Bestimmung stellt sicher, dass die ausserhalb einer Plattform übermittelten Akten nicht nur an ihrem Destinationsort, sondern auch auf dem Transportweg vor unberechtigter Kenntnisnahme und Veränderung geschützt sind.

Art. 24 Elektronische Übermittlung unter Behörden

Auch Zustellungen unter Behörden, einschliesslich Gerichten und Amtsstellen im Sinn von Artikel 128c Absatz 2 ZPO, können ausserhalb einer Plattform nach dem BEKJ erfolgen. Mit dem BEKJ wird bei der elektronischen Kommunikation ein für alle Parteien nachvollziehbarer Verfahrensablauf erreicht, in dem bei allen relevanten Handlungen eine Quittung erstellt wird, welche ein geregeltes elektronisches Siegel enthält. Diese Nachvollziehbarkeit darf nicht durch die in den Prozessgesetzen festgelegte Ausnahme umgangen werden.

Dieser Artikel fordert daher ebenfalls als Voraussetzung, dass die Nachvollziehbarkeit gewährleistet wird, indem die Namen, die Grösse und die Hashwerte der übermittelten Dokumente wie auch die Zeitpunkte unveränderbar aufgezeichnet werden.

Abgrenzung zu direkten Datenbankabfragen

Die zuständige Behörde prüft ferner, ob es sich bei einer vorgesehenen Tätigkeit überhaupt um eine Zustellung nach dem BEKJ handelt. Dies ist zu verneinen, wenn eine direkte Datenbankabfrage bei einer anderen Behörde getätigt wird. Beispiele für direkte Datenbankabfragen sind Personenkontrollen mit Identitätsabfragen mit dem Abfragesystem MACS (Multiple Applications Coordination Services) oder die Fahrzeugüberprüfungen mit dem Informationssystem Verkehrszulassung. In beiden Fällen können die Polizeien direkt Datenbankabfragen tätigen.

2. Abschnitt: Elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Art. 25

Im Bereich des SchKG hat sich das «eSchKG» über Sedex etabliert. Sedex ist eine sichere Plattform für den elektronischen Datenaustausch in der Schweiz, die vom Bund betrieben und überwacht wird. Im Bereich des Schuldbetreibungs- und Konkursgesetzes wird Sedex im Rahmen des Projekts «eSchKG» (elektronisches SchKG) genutzt. Damit werden Betreibungsdaten wie Zahlungsbefehle, Pfändungsurkunden oder Verwertungsbegehren verschlüsselt und automatisiert zwischen Gläubigern, Schuldnern und Betreibungsämtern ausgetauscht. Im Jahr 2024 wurden 2 598 112 Betreibungen und 878 919 Registerauszüge via «eSchKG»/Sedex übermittelt.

Die Bestimmung zum «eSchKG» befand sich bisher in der VeÜ-ZSSV. Der Inhalt dieser Bestimmung wurde mit dem BEKJ auf Gesetzesstufe gehoben und ist neu in Artikel 33b SchKG i.d.F. des BEKJ geregelt. Im Rahmen des VE-VEKJ ist es somit ausreichend, wenn die entsprechende Regelungskompetenz an das EJPD delegiert werden. Damit besteht weiterhin eine ausreichende Grundlage für die Verordnung des

EJPD vom 9. Februar 2011²² über die elektronische Übermittlung im Betreibungsweisen.

In Absatz 2 wird die spezifische eSchKG-Terminologie mit Postfächern verwendet. Der Begriff Postfach ist nicht im Sinne von E-Mail-Postfächern verstanden, sondern als elektronische, rechtlich verbindliche Zustell- und Empfangsstellen.

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

Art. 26

Abs. 1

Die bestätigenden Parteien müssen ihre Bestätigung persönlich und manuell vornehmen, ohne dass Dritte oder Automatismen eingreifen. Dies wird durch die «Eigenhändigkeit» betont. Dadurch verhindert man, dass Bestätigungen kopiert oder gefälscht werden, und stellt sicher, dass die bestätigende Person physisch anwesend ist.

Abs. 2

Das Gerät muss nicht nur den genauen Zeitpunkt der Bestätigung protokollieren, sondern auch biometrische Details erfassen. Dazu gehören die Beschaffenheit der Striche (z. B. Dicke und Form), die Druckstärke, der Fluss der Bewegung (z. B. Geschwindigkeit) und die Richtung der Bewegungen. Diese Daten sind fest mit der Bestätigung zu verknüpfen. Es geht dabei um eine forensische Nachverfolgbarkeit: Diese Daten machen die Bestätigung einzigartig und überprüfbar, vergleichbar mit einer graphologischen Analyse einer Handschrift.

Abs. 3

Nach der ersten Bestätigung wird das Gerät so konfiguriert, dass keine Modifikationen am Protokoll mehr möglich sind – mit Ausnahme des Hinzufügens weiterer Bestätigungen (z. B. von anderen Beteiligten). Dadurch wird das Protokoll unveränderlich. Dies verhindert Nachbesserungen oder Fälschungen und es schützt die Integrität.

Abs. 4

Diese Bestimmung legt fest, dass Protokolle, die ausschliesslich Behördenmitgliedern unterzeichnen müssen, auch auf elektronischem Weg rechtsgültig bestätigt werden können. Konkret gelten geregelte elektronische Siegel oder qualifizierte elektronische

²² SR 281.112.1

Signaturen als gleichwertige elektronische Bestätigungen im Sinn eines «elektronischen Geräts» gemäss den relevanten Verfahrensgesetzen.

4. Kapitel: Schlussbestimmungen

Art. 27 *Aufhebung und Änderung anderer Erlasse*

Der Anhang 1 enthält die Liste der Erlasse, die mit der Inkraftsetzung des VE-VEKJ aufgehoben oder geändert werden.

Art. 28 *Inkrafttreten*

Diese Bestimmung enthält das Datum, an dem die Verordnung in Kraft tritt.

4 Erläuterungen zu Anhang 1 (Aufhebung und Änderung anderer Erlasse)

4.1 Aufhebung der Verordnung vom 18. Juni 2010²³ über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV)

Die gesetzliche Grundlage für die VeÜ-VwV liegt in den heutigen Bestimmungen über die elektronische Eingabe im VwVG. Mit der abschliessenden Inkraftsetzung des BEKJ fallen die bisherigen Regelungen weg und an deren Stelle treten neue Bestimmungen. Die bisherige VeÜ-VwV ist infolge Wegfallens der gesetzlichen Grundlagen aufzuheben.

4.2 Aufhebung der Verordnung vom 18. Juni 2010²⁴ über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV)

Vgl. Ausführungen zu Ziffer 4.1.

²³ SR 172.021.2

²⁴ SR 272.1

4.3 Verordnung vom 23. November 2016²⁵ über die elektronische Signatur

Art. 14a Vom Validator zu prüfende Signaturen und Siegel

Abs. 1

Diese Bestimmung schränkt die Pflicht zur Prüfung auf qualifizierte elektronische Signaturen, geregelte elektronische Siegel und qualifizierte elektronische Zeitstempel ein, da nur diesen Signaturen eine gesetzliche Rechtswirkung haben. Darüber hinaus kann der Validator weitere elektronische Signaturen prüfen, die für sinnvoll erachtet werden wie z. B. das Klasse-B-Zertifikat der Bundesverwaltung.

Abs. 2

Am 29. Januar 2025 hat der Bundesrat das UVEK (BAKOM) zusammen mit dem EDA beauftragt, ein Verhandlungsmandat mit der EU über eine gegenseitige Anerkennung der elektronischen Signaturen auszuarbeiten. Im Hinblick auf dieses Verhandlungsmandat sind Befürchtungen entstanden, dass der Validator zur Prüfstelle für die gesamte EU wird. Diese Bestimmung legt fest, dass eine explizite Prüfpflicht für gegenseitig anerkannte Signaturen in den betreffenden internationalen Abkommen enthalten sein muss; andernfalls prüft der Validator lediglich Signaturen nach Schweizer Recht.

Abs. 3

Bei Dokumenten mit mehreren Signaturen oder Siegeln muss der Validator detailliert zurückmelden, welche davon den ZertES-Anforderungen oder internationalen Abkommen genügen. Statt einer pauschalen Bewertung erhält die Nutzerin oder der Nutzer (z. B. eine Behörde) eine Aufschlüsselung, welche Elemente gültig sind und welche nicht. Dies erleichtert die Bearbeitung komplexer Dokumente wie Verträge mit mehreren Parteien, verhindert Missverständnisse und hilft bei der Entscheidungsfindung, ob ein Dokument als Ganzes akzeptiert werden kann. Der Validator gibt jedoch keine Auskunft über die Rechtswirkung eines geprüften Dokuments.

Abs. 4

Der Validator kann bei der Verwendung eines Behördensiegels mitteilen, dass es sich um ein Dokument einer Behörde handelt und zu welchem Zweck es ausgestellt wurde. Zum Beispiel ob es sich um eine amtliche Meldung, Dokumente der Publikationsplattform des Bundes, einen Strafregistrauszug oder Ähnliches handelt. Soweit der Validator dies tut, erleichtert dies die Einordnung der geprüften Dokumente und kann eine Effizienzsteigerung bewirken.

²⁵ SR 943.032

Es hat sich gezeigt, dass ein Hauptproblem bei der Validierung von elektronischen Signaturen darin liegt, dass die internationalen technischen Normen viel Spielraum bieten. Dies führt zu Problemen, weil nicht jede einzelne Implementierung berücksichtigt werden kann. Diese Bestimmung ermöglicht es dem BAKOM, den Validierungsprozess klar zu regeln und somit die Schaffung einheitlicher Standards zu fördern, die sicherstellen, dass Validierungen zuverlässig und reproduzierbar sind. Diese Kann-Bestimmung ist nicht so zu verstehen, dass das BAKOM mit Erlass dieser Verfügung einen Auftrag erhält, den Validierungsprozess zu regeln.

Sollte es sich als notwendig herausstellen, dass das BAKOM Regelungen zum Validierungsprozess erarbeitet, wird es dabei internationale Standards einbeziehen und nur dort Regelungen treffen, wo die internationalen Standards keine klaren Vorgaben aufweisen.

5 Erläuterungen zu Artikel 26 Absatz 5 BEKJ

Artikel 26 Absatz 5 BEKJ wurde während der parlamentarischen Beratungen eingefügt und in der Botschaft bisher noch nicht erläutert. Im Rahmen der parlamentarischen Diskussionen wurde seitens des Bundesrates in Aussicht gestellt, diese Bestimmung noch zu erläutern. Was hiermit erfolgt.

Das Anliegen war, dass es neben der Möglichkeit des Artikels 26 Absatz 1 BEKJ noch eine weitere Möglichkeit der Fristwahrung gibt, da Artikel 26 Absatz 1 BEKJ nicht alle Fälle abdecken kann, z. B. bei einer bevorstehenden Ferienabwesenheit, weshalb die erneute Erreichbarkeit nicht abgewartet werden kann.

Nach Artikel 26 Absatz 5 BEKJ wird die Frist deshalb ebenfalls gewahrt, wenn die gesamte Eingabe in Papierform der Post oder einer diplomatischen oder konsularischen Vertretung übergeben wird.

Ist die Eingabe samt Beilagen umfangreich, kann diese nach Schliessung der Post möglicherweise nicht mehr in einen Briefkasten eingeworfen werden. Artikel 26 Absatz 5 BEKJ sieht deswegen vor, dass die Frist ebenfalls gewahrt wird, wenn die Existenz der einzureichenden Dokumente bewiesen wird. Man kann dies mittels einer Hashsumme der Dokumente erreichen, die man im Schreiben mitübersendet – also ähnlich, wie das in den Eingangsquittungen aufgeführt ist. Dies befreit aber nicht vom rechtzeitigen Einwurf im Briefkasten oder Übergabe an eine diplomatische oder konsularische Vertretung. Dabei ist darauf zu achten, dass ein sicherer Hashalgorithmus verwendet wird. Beispiele sind: SHA-256, SHA-512, SHA-3, BLAKE2 und BLAKE3. Veraltete Algorithmen wie MD5 oder SHA-1 sollten nicht verwendet werden, da diese nicht mehr sicher sind.

6 Auswirkungen

6.1 Auswirkungen auf den Bund

Der VE-VEKJ hat keine zusätzlichen personellen Auswirkungen, die über den bereits in Ziff. 6.1 der Botschaft zum BEKJ geschilderten Ressourcenbedarf hinausgehen. In finanzieller Hinsicht ist auszuführen, dass bereits die Botschaft darauf hingewiesen hat, dass Kosten für den Betrieb und die Weiterentwicklung über Gebühren finanziert und mittel- bis langfristig durch Kosteneinsparungen mindestens kompensiert werden können.

Darüber hinaus müssen die Verwaltungseinheiten des Bundes sowohl bei der zentralen Plattform wie auch der allgemeinen Plattform für Verwaltungsverfahren ein Organisationskonto eröffnen und – soweit nicht über die Schnittstelle angebunden – regelmässig prüfen müssen.

6.2 Auswirkungen auf Kantone und Gemeinden

Die Ausführungen zu Ziffer 6.1 gelten gleichermassen für die Kantone und Gemeinden mit der Einschränkung, dass nur die Gerichte, Staatsanwaltschaften und Polizeien auf der zentralen Plattform ab Inkrafttreten über ein Konto verfügen müssen. Die übrigen kantonalen Behörden können ein Onboarding bei Bedarf vornehmen, d. h. wenn sie erstmals mit Gerichten, Staatsanwaltschaften, Polizeien oder Verwaltungseinheiten des Bundes kommunizieren müssen.

Darüber hinaus müssen die Kantone gegebenenfalls ihre gesetzlichen Grundlagen anpassen, falls sie bisher auf die VeÜ-VwV oder die VeÜ-ZSSV verwiesen haben. Diese Verordnungen werden mit der Inkraftsetzung des VE-VEKJ aufgehoben.

6.3 Auswirkungen auf die Volkswirtschaft

Die Digitalisierung schreitet voran. Immer mehr Geschäfte können online abgewickelt werden. 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.

Sichere und geregelte Verhältnisse auch im Cyberraum tragen wesentlich zur Attraktivität des Wirtschaftsstandorts Schweiz und zu seiner Wettbewerbsfähigkeit bei. Der Bundesrat verfolgt das Ziel, auf Seiten des Staates die Beiträge zu leisten, die es für einen erfolgreichen Übergang der Schweiz in die Informationsgesellschaft braucht. Er hat dazu zahlreiche Massnahmen beschlossen, die meist entweder die Anpassung des gesetzlichen Rahmens oder die Bereitstellung von Infrastrukturelementen betreffen. Dazu gehören beispielsweise das ZertES sowie die Schaffung von einheitlichen Personen- und Unternehmens-Identifikationsnummern und der entsprechenden Register. Mit dem BEKJ geht der Bundesrat nun noch einen Schritt weiter, indem zukünftig die Gerichte, Behörden sowie professionelle Rechtsanwenderinnen und -an-

wender einem Obligatorium für den elektronischen Rechtsverkehr unterworfen werden. Dazu wird eine sichere und einfach zu bedienende Plattform geschaffen, deren Benutzung auch attraktiv sein wird für Personen und Unternehmen, die dem Obligatorium nicht unterstehen. Mit dieser Plattform können Verfahren vollständig elektronisch abgewickelt werden, was eine effiziente Rechtspflege begünstigt.

Die Anwaltschaft ist vom Obligatorium besonders stark betroffen. Sie wird zukünftig Rechtsschriften und Beilagen den Gerichten und (Strafverfolgungs-) Behörden nur noch elektronisch einreichen können. Dies führt zu einer Änderung der Arbeitsweise, die jedoch nicht zwangsläufig zu Mehrkosten führt. Mögliche Mehrkosten könnten durch notwendige Anpassungen der Infrastruktur, veränderten Personalbedarf oder erhöhten Zeitaufwand entstehen.

6.4 Auswirkungen auf die Gesellschaft

Der VE-VEKJ hat wenig unmittelbare Auswirkungen auf die Gesellschaft.

Für Personen, die dem Obligatorium nicht unterstehen, bleibt der bisherige Ablauf in der Kommunikation mit der Justiz unverändert. Diese Personen können weiterhin mit Gerichten und Behörden auf dem postalischen Weg kommunizieren. Neu ist allerdings, dass sie ebenfalls einfach und sichere elektronisch mit Gerichten und Behörden kommunizieren können und so auch von den Vorteilen des elektronischen Rechtsverkehrs profitieren. Diesbezüglich trifft jede Person selbst die Entscheidung. Um vom elektronischen Rechtsverkehr zu profitieren, benötigen sie lediglich einen Internetanschlusses, ein Konto auf der zentralen Plattform beziehungsweise der allgemeinen Verwaltungsplattform für Verwaltungsverfahren und eine Registrierung beim Behörden-Login AGOV.

Professionelle Rechtsanwenderinnen und Rechtsanwender haben dieselben Voraussetzungen.

7 Rechtliche Aspekte

7.1 Informationssicherheit

Der Missbrauch von Informationen und die Störung der zentralen Plattform können wesentliche Interessen der Schweiz und die Rechte von Personen schwerwiegend beeinträchtigen. Sie gefährden zudem die gesetzliche Aufgabe für den Betrieb der zentralen Plattform wie auch der Plattform für das allgemeine Verwaltungsverfahren. Das ISG und die Informationssicherheitsverordnung vom 8. November 2023 (ISV)²⁶ bilden die Grundlage für die bestmögliche Sicherstellung der Informationssicherheit.

²⁶ SR 128.1

Der VE-VEKJ braucht keine detaillierte Regelung zum Umgang mit Gefährdungen der Informationssicherheit. Denn das ISG und die ISV bieten bereits die notwendigen rechtlichen Grundlagen. Ähnlich wie beim DSG wird auch hier auf die bestehende Systematik des Rechts hingewiesen. Das bedeutet, dass die bestehenden Regelungen in den relevanten Gesetzen bereits ausreichend sind, um den sicheren Umgang mit potenziellen Risiken in der Informationssicherheit zu gewährleisten.

7.2 Datenschutz

Auf die zentrale Plattform sowie die Plattform für allgemeine Verwaltungsverfahren ist grundsätzlich das DSG und die zugehörigen Verordnungen anwendbar. Das anwendbare Verfahrensrecht regelt für laufende Verfahren die Bearbeitung von Personendaten und die Rechte der betroffenen Personen (Art. 2 Abs. 3 DSG). Der VE-VEKJ verzichtet auf Verweise zu DSG-Bestimmungen, um Wiederholungen zu vermeiden und die Auslegung zu erleichtern. Die Ausführungsbestimmungen konzentrieren sich auf den im BEKJ geschaffenen Rahmen für die Bearbeitung, Aufbewahrung und Löschung von Daten.