Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bern, 20. Juni 2025

Entwurf E-ID-Verordnung

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

BJ-D-4ED93401/161

Übersicht

Mit der Verordnung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Verordnung, VEID) werden unter anderem die Verfahren und Zuständigkeiten für die Ausstellung und Verwendung der E-ID präzisiert. Darüber hinaus wird die staatliche Vertrauensinfrastruktur definiert, die sowohl von Behörden als auch von privaten Akteurinnen genutzt werden kann, um elektronische Nachweise sicher auszustellen und zu verifizieren. Ziel der Verordnung ist es, eine klare und sichere Grundlage für den Umgang mit der E-ID und anderen digitalen Nachweisen zu schaffen.

Ausgangslage

Nach der Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste in der Volksabstimmung vom 7. März 2021 beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement, gemeinsam mit der Bundeskanzlei und dem Eidgenössischen Finanzdepartement, mit der Entwicklung eines sicheren staatlichen elektronischen Identitätsnachweises. Am 13. Juni 2022 stimmten Nationalrat und Ständerat sechs Motionen zu, die die Schaffung eines staatlichen elektronischen Identifikationsnachweises forderten. Am 22. November 2023 verabschiedete der Bundesrat den Gesetzesentwurf über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID). Ziel ist die Einführung einer kostenlosen und freiwilligen E-ID, die Nutzerinnen und Nutzern eine sichere und unkomplizierte digitale Identifikation ermöglicht. Die E-ID wird vom Bund herausgegeben und gewährleistet maximalen Schutz der Personendaten insbesondere durch Datensparsamkeit. Im Sinne der digitalen Selbstbestimmung ist die Ausstellung und der Einsatz der E-ID freiwillig. Zudem wird den Inhaberinnen und Inhabern die Kontrolle über ihre Daten ermöglicht. Neben der E-ID wird auch an der Digitalisierung anderer Nachweise gearbeitet. Der Bund stellt die erforderliche Vertrauensinfrastruktur bereit, einschliesslich einer elektronischen Brieftasche, einer Anwendung zur Nachweisüberprüfung sowie Basis- und Vertrauensregistern. Diese Infrastruktur kann auch von Privaten genutzt werden, die elektronische Nachweise ausstellen und verifizieren möchten. In der Schlussabstimmung vom 20. Dezember 2024 wurde das BGEID vom Parlament mit deutlicher Mehrheit verabschiedet (Nationalrat: Für Annahme des Entwurfes 170 Stimmen, dagegen 25 Stimmen [1 Enthaltung]; Ständerat: Für Annahme des Entwurfes 43 Stimmen, dagegen 1 Stimme [0 Enthaltungen]). Das Referendum ist am 7. Mai formell zustande gekommen. Die Abstimmung über das BGEID findet am 28. September 2025 statt.

Wenn das Volk das BGEID nicht ablehnt, kann dieses frühestens Mitte 2026 in Kraft gesetzt werden. Bis zu diesem Zeitpunkt müssen auch die Ausführungsbestimmungen vom Bundesrat verabschiedet werden können. Dies ist aber nur möglich, wenn mit der Eröffnung der Vernehmlassung nicht bis nach der Referendumsabstimmung zugewartet wird.

Inhalt der Vorlage

Das BGEID soll den Einwohnerinnen und Einwohnern der Schweiz sowie den Schweizerinnen und Schweizern im Ausland die Möglichkeit zur Verfügung stellen, sich künftig sicher, schnell und unkompliziert digital auszuweisen. Der Verordnungsentwurf konkretisiert die Umsetzung des BGEID und regelt insbesondere die Vertrauensinfrastruktur, die E-ID und die damit verbundenen technischen sowie organisatorischen Aspekte der elektronischen Nachweise. Die Vertrauensinfrastruktur ist für alle elektronischen Nachweise gedacht und umfasst das Basisregister, in dem Identifikatoren eingetragen werden, das Vertrauensregister zur Bestätigung dieser Identifikatoren sowie Anwendungen zur Aufbewahrung und Überprüfung elektronischer Nachweise. Der Vernehmlassungsentwurf regelt die Eintragung, Nutzung und Löschung von Informationen zu elektronischen Nachweisen durch natürliche und juristische Personen.

Die E-ID wird online beantragt, wobei das Bundesamt für Polizei (fedpol) für die Ausstellung verantwortlich ist. Die Identitätsprüfung kann entweder online oder vor Ort in den kantonalen Erfassungszentren oder – für die Auslandschweizerinnen und -schweizer – bei der zuständigen konsularischen Vertretung der Schweiz erfolgen. Die online-Identitätsprüfung wird gestartet durch das Fotografieren des Ausweisdokuments und eine Videoaufnahme des Gesichts, die automatisiert überprüft werden. Diese Videoausschnitte werden mit dem Gesichtsbild verglichen, das in den Informationssystemen nach Artikel 17 Absatz 2 BGEID (z.B. Informationssystem Ausweisschriften) gespeichert ist. Bei Übereinstimmung erhält die Antragstellerin oder der Antragsteller die E-ID direkt auf das Endgerät. In den Kantonen und in den konsularischen Vertretungen der Schweiz im Ausland, die eine Identitätsprüfung vor Ort durchführen, kann das Verfahren variieren.

Wichtige technische Details, wie das Format und die Standards der elektronischen Nachweise, werden als Empfehlungen veröffentlicht, können aber teilweise verbindlich erklärt werden.

Inhaltsverzeichnis

Erläuternder Bericht

1 Grundzüge der Vorlage

Mit dem BGEID sollen den Einwohnerinnen und Einwohnern der Schweiz sowie den Schweizerinnen und Schweizern im Ausland ihre digitale Identität und weitere digitale Nachweise rasch und in einer hohen Qualität und sicher zur Verfügung gestellt werden. Mit dem vorliegenden Verordnungsentwurf wird die Umsetzung des BGEID konkretisiert. Er regelt insbesondere die Vertrauensinfrastruktur und die E-ID sowie die Umsetzung der technischen und organisatorischen Aspekte zur Verwendung elektronischer Nachweise im Allgemeinen.

1.1 Vertrauensinfrastruktur

Gemäss dem BGEID sind die Bestandteile der Vertrauensinfrastruktur nicht nur für die E-ID gedacht, sondern grundsätzlich für alle kompatiblen elektronischen Nachweise. Er umfasst:

- das Basisregister, in dem Ausstellerinnen von elektronischen Nachweisen die erforderlichen Angaben wie ihre Identifikatoren eintragen können;

- das Vertrauensregister, das als System zur Bestätigung von Identifikatoren aus dem Basisregister dient;

- die Anwendung zur Aufbewahrung und zum Vorweisen von elektronischen Nachweisen und das System für Sicherungskopien; und

- die Anwendung zur Überprüfung von elektronischen Nachweisen.

Der Verordnungsentwurf führt im Allgemeinen die Eintragung und Nutzung bzw. Löschung aus der Vertrauensinfrastruktur näher aus. Die Eintragung, Benutzung und Löschung gelten für alle interessierten natürlichen und juristischen Personen, die elektronische Nachweise ausstellen und nutzen möchten.

1.2 Antrags- und Ausstellungsverfahren bezüglich der E-ID

Der Verordnungsentwurf konkretisiert ferner die Beantragung, die Identitätsprüfung, die Ausstellung und den Widerruf der vom Bund ausgestellten E-ID. Die E-ID wird online beantragt und die Identitätsprüfung kann entweder online oder vor Ort in den kantonalen Erfassungszentren oder – für die beim Konsulat registrierten Auslandschweizerinnen und -schweizer – bei der zuständigen konsularischen Vertretung der Schweiz erfolgen. Für die Ausstellung der E-ID ist das fedpol zuständig.

In einem ersten Schritt wird die Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen des Bundes (staatliche elektronische Brieftasche, Bundes-Wallet) auf dem Endgerät der antragstellenden Person installiert, z. B. auf einem Mobilgerät. In einem zweiten Schritt fotografiert die Antragstellerin oder der Antragsteller

den amtlichen Ausweis (Identitätskarte, Pass, Ausländerausweis), und macht eine Videoaufnahme vom Gesicht. Die Daten werden mittels der Anwendung der staatlichen Prüfstelle zur Überprüfung zugestellt. Grundsätzlich soll diese Überprüfung automatisiert erfolgen. Stimmen die eingereichten Daten mit dem staatlichen Ausweisregister überein, erhält die antragstellende Person die E-ID umgehend auf das Endgerät zugestellt. Die Ausstellung der E-ID kann gleichzeitig in mehrere Anwendungen auf einem oder mehreren Endgeräten erfolgen. Dieser Vorgang sollte insgesamt nur wenige Minuten dauern. Es ist damit zu rechnen, dass bei der Einführung der E-ID allerdings mit längeren Wartezeiten zu rechnen ist (Queuing-System). Das System zur Ausstellung wird vor dem Hintergrund der Qualitätssicherung schrittweise ausgebaut.

Sofern eine Identitätsprüfung vor Ort erfolgt, kann das Verfahren zur Identitätsprüfung auch in einem kantonalen Erfassungszentrum oder bei der konsularischen Vertretung stattfinden. Da die Umsetzung des Identitätsprüfungsverfahrens vor Ort in der Verantwortung der Kantone und des Bundes (für die Vertretungen der Schweiz im Ausland) liegt, ist in diesem Zusammenhang mit Unterschieden beim Verfahren auszugehen.

1.3 Technische Angaben

Für eine sichere Verwendung der E-ID werden die technischen Anforderungen der E-ID näher ausgeführt. Das Eidgenössische Justiz- und Polizeidepartement (EJPD) legt das technische Format und die Attribute für die Datenübermittlung, die Anforderungen an die Schnittstelle zum Informationssystem für die Ausstellung und den Widerruf der E-ID sowie die Standards und Protokolle für die Datenübermittlung bei der Ausstellung der E-ID fest.

Folgende technische Angaben werden in erster Linie als Empfehlungen (Artikel 33 und 34) veröffentlicht: das Format der elektronischen Nachweise, der Standards und Protokolle für die Kommunikationsvorgänge beim Ausstellen und Vorweisen elektronischer Nachweise. Das EJPD kann vorsehen, dass Empfehlungen oder Teile davon als verbindlich erklärt werden (Artikel 35).

2 Rechtsvergleich mit dem europäischen Recht

In der EU sind im Bereich der digitalen Identität Reformen im Gange. Der Bundesrat ist der Ansicht, dass diese Entwicklungen in die Überlegungen auf nationaler Ebene einbezogen werden sollten. Am 3. Juni 2021 verabschiedete die Europäische Kommission einen Vorschlag zur Änderung der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) und zur Schaffung eines rechtlichen Rahmens für eine europäische elektronische Identität. Im Rahmen dieser neuen Verordnung ist vorgesehen, dass die Mitgliedstaaten den Bürgerinnen und Bürgern innerhalb von 24 Monaten nach ihrem Inkrafttreten elektronische Brieftaschen zur Verfügung stellen, in denen diese ihre nationale elektronische Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerausweis, Abschlusszeugnisse, Bankkonto) verknüpfen können. Die Brieftaschen können von Behörden oder privaten Einrichtungen bereitgestellt werden, sofern diese von den Mitgliedstaaten anerkannt sind.

Am 30. April 2024 verabschiedete der Europäische Rat die vorgeschlagene Änderung der eIDAS-Verordnung. Der von der Kommission vorgegebene Rahmen basiert auf den Grundsätzen von Self-Sovereign Identity (SSI). Er ist aber technologisch neutral, wenn es um die genaue Umsetzung dieser Grundsätze geht. Zwischen dem 12. August 2024 und dem 9. September 2024[1] sowie zwischen dem 29. November 2024 und dem 2. Januar 2025 eröffnete die Kommission die Konsultation für jeweils fünf Entwürfe zu Durchführungsverordnungen der EU-Kommission, die dazu dienen, die verabschiedeten Änderungen der eIDAS-Verordnung umzusetzen. Die Umsetzungsakte beziehen sich insbesondere auf technische Standards, Verfahrensfragen und Formate, um die Interoperabilität, das Vertrauen und die Rechtssicherheit in den EU-Mitgliedsstaaten zu gewährleisten. Sie befassen sich unter anderem mit Sicherheitsvorfällen im Zusammenhang mit elektronischen Brieftaschen, der grenzüberschreitenden Verwendung elektronischer Identitäten sowie der Registrierung und Führung einer Liste der Ausstellerinnen und Verifikatorinnen sowie der elektronischen Brieftaschen.

Im Vergleich zur EU verfolgt die Schweiz einen weniger regulierten Ansatz, der mehr Raum für Innovationen lässt. So verzichtet die Schweiz auf formelle und teure Zulassungsverfahren sowie auf die Führung von Listen. Die Schweiz ist rechtlich nicht verpflichtet, die eIDAS-Verordnung sowie die dazu gehörenden Änderungen und Umsetzungsakte zu übernehmen. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten Mitgliedsländern der EU hat sie jedoch ein Interesse daran, ihr System für den elektronischen Identitätsnachweis so zu gestalten, dass es interoperabel mit jenem der EU ist. Das BGEID sieht vor, dass der Bundesrat internationale Abkommen abschliessen kann, um eine internationale Anerkennung der E-ID zu erreichen und ausländische E-ID zu anerkennen (Artikel 32 BGEID). Die vorliegende Verordnung berücksichtigt die Entwicklung in der EU und ist nicht so auszulegen, dass sie der Kompatibilität der elektronischen Identifizierung mit dem europäischen Recht entgegensteht.

3 Erläuterungen zu einzelnen Artikeln

Ingress

Der vorliegende Verordnungsentwurf stützt sich auf verschiedene Artikel des BGEID. Die Artikel 2 Absatz 5 Buchstabe a, Artikel 3 Absatz 7, Artikel 4, Artikel 8 Absätze 2 und 3, Artikel 9 Absatz 2, Artikel 17 Absatz 1, Artikel 18 Absätze 5 und 6, Artikel 20, Artikel 21, Artikel 28 Absatz 4, Artikel 30, Artikel 31 Absatz 5, Artikel 33 und Artikel 35 Absatz 2 BGEID werden aber im Ingress nicht einzeln genannt.

[1] Durchführungsverordnungen der EU-Kommission (2024/2977, 2024/2979, 2024/2980, 2024/2981, 2024/2982) angenommen am 4. Dezember 2024.

1. Kapitel: Gegenstand

Art. 1

Insgesamt zielt die Verordnung darauf ab, den reibungslosen und sicheren Betrieb der Vertrauensinfrastruktur und der E-ID als elektronischer Nachweis zu garantieren und dabei sowohl Sicherheit (insbesondere Vertrauenswürdigkeit) als auch Inklusion zu wahren. Dies wird durch technische Bedingungen und Verfahrensregeln gewährleistet. Ein Fokus liegt dabei auf der Sicherheit, um Missbrauch oder Manipulation zu verhindern und Vertrauen in das System zu schaffen und zu bewahren.

Die Verordnung regelt die Grundregeln für die Errichtung und den Betrieb der Register und der Anwendungen zur Aufbewahrung und Vorweisung (elektronische Brieftasche)[2] sowie zur Überprüfung von elektronischen Nachweisen (Check-App des Bundes) (Buchstabe a). Die Verordnung regelt ferner den gesamten Prozess rund um die elektronische Identität (E-ID). Dazu gehören der Antrag auf Ausstellung, die Überprüfung der Identität der antragstellenden Person, die eigentliche Ausstellung sowie die Bedingungen, unter denen eine E-ID widerrufen werden kann (Buchstabe b). Sodann wird festgelegt, wie personenbezogene Daten aufbewahrt und wann bzw. wie sie gelöscht werden müssen. Dies betrifft insbesondere die Daten, die im Zusammenhang mit einer E-ID und anderen elektronischen Nachweisen erhoben werden (Buchstabe c).

2. Kapitel: Vertrauensinfrastruktur

Die Vertrauensinfrastruktur und weitere dazugehörende Dienste sind eine Fachanwendung des Bundesamtes für Justiz (BJ). Das BJ tritt als Auftraggeber gegenüber dem Bundesamt für Informatik und Telekommunikation (BIT) auf und trägt die Gesamtverantwortung.

1. Abschnitt: Portal zur Bearbeitung von Registerdaten

Art. 2 Zweck und Betrieb

Damit Einträge im Basis- und Vertrauensregister möglich sind, wird für Ausstellerinnen und Verifikatorinnen von elektronischen Nachweisen ein elektronisches Portal zur Verfügung gestellt (Portal). Dieses Portal soll ähnlich wie bei anderen Registrierungsplattformen die erforderlichen Daten für die Eintragung in den Registern abfragen. Das BJ ist zuständig für das Portal.

Die Registrierung erfolgt dabei über das vom Eidgenössischen Finanzdepartement bereitgestellte e-Portal. Dort steht eine dedizierte Anwendung zur Verfügung, über die die

[2] Die elektronische Brieftasche trägt den geschützten Namen «swiyu».

Ausstellerinnen und Verifikatorinnen sämtliche Tätigkeiten ausführen sowie die Gebühren bezahlen können. Mittelfristig soll das Once-Only-Prinzip durch die Integration in andere Portale resp. die Verknüpfung mit bestehenden Datensätzen realisiert werden.

Art. 3 Bei der Registrierung erfasste Daten

Absatz 1

Für die Registrierung müssen Ausstellerinnen und Verifikatorinnen von elektronischen Nachweisen folgende Angaben erfassen:

- Wenn sie eine natürliche Person ist: Vorname(n) und Name(n)
- Wenn sie eine juristische Person oder Personengesellschaft ist:
    - Firma, Sitz und Unternehmens-Identifikationsnummer (UID) gemäss dem Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer[3];
    - Adresse;
    - E-Mail-Adresse;
    - Telefonnummer;
    - Zahlungsinformationen.

Mittelfristig wird geprüft, ob das UID-Register direkt als Datenlieferant herangezogen werden kann. Während der Vernehmlassung wird geprüft, ab wann diese Schnittstelle umsetzbar wäre. Ausserdem wird ein Abgleich mit dem eidgenössische Gebäude- und Wohnungsregister evaluiert, damit auch Angaben wie der Sitz einer juristischen Person oder Personengesellschaft automatisiert übernommen werden kann. Gemäss Artikel 15*a* der Verordnung vom 9. Juni 2017 über das eidgenössische Gebäude- und Wohnungsregister[4] teilt das BJ fehlerhafte Daten dem Bundesamt für Statistik mit.

Absatz 2

Die Adresse, Telefonnummer, E-Mail-Adresse oder sonstige Kontaktangaben für die Registration werden in den Registern nicht erfasst, sondern beim BIT gespeichert. Diese Daten sind nicht öffentlich einsehbar und dienen allein zur Registrierung und Verwaltung der Stammdaten resp. der Geschäftskundenbeziehung im System. Die Erhebung von Zahlungsinformationen ist erforderlich, da von den Ausstellerinnen und Verifikatorinnen Gebühren für die Daten erhoben werden, die sie in das Basisregister eintragen, sowie für die Daten, deren Eintragung in das Vertrauensregister sie beantragen (Artikel 38). Es sind ausschliesslich direkte Abrechnungsmittel mit Hilfe von «So-

[3] SR **431.03**

[4] SR **431.841**

fort-Zahlungsdiensten» (z. B. mittels Kreditkarten) vorgesehen. Damit sollen aufwändige Prüfprozesse, allfällige Löschung aus den Registern und Inkassoverfahren verhindert werden.

2. Abschnitt: Basisregister

Art. 4 Inhalt

Die Ausstellerin oder Verifikatorin von elektronischen Nachweisen verfügt nach der Registrierung auf dem Portal Zugang zum Basisregister. Sie kann über eine technische Schnittstelle Daten im Basisregister eintragen, die dazu dienen, die Authentizität und Integrität ihrer ausgestellten elektronischen Nachweise sicherzustellen. Zu diesen Daten gehören öffentliche kryptografische Schlüssel und Angaben zu den widerrufenen elektronischen Nachweisen. Die Ausstellerin erhält einen geschützten Zugang zum Basisregister, damit sie ihre widerrufenen Nachweise verwalten kann. Neben Ausstellerinnen können auch Verifikatorinnen Daten im Basisregister eintragen. Die Ausstellerin oder Verifikatorin erhält bei der Eintragung ihrer Daten einen anonymen identifizierbaren Kennwert (Identifikator). Ihren jeweiligen Identifikator generiert sie durch ein technisches Zusammenspiel mit dem BIT. Für die Verwaltung der eingetragenen Daten ist sie selbst verantwortlich. Aus dem Identifikator sind keine personenbezogenen Rückschlüsse auf die Ausstellerin oder Verifikatorin möglich.

Die Inhalte des Basisregisters sind für die Öffentlichkeit zugänglich. Der Abruf der öffentlichen Daten ist über eine Schnittstelle ohne Registrierung möglich und für die Überprüfung der kryptografischen Gültigkeit elektronischer Nachweise notwendig. Die von einer Ausstellerin oder Verifikatorin im Basisregister eingetragenen Daten sind vor der Bearbeitung durch Dritte geschützt, so dass insbesondere nur die Ausstellerin oder Verifikatorin die Daten bearbeiten kann und sichergestellt ist, dass die Echtheit der Daten jederzeit gewährleistet ist.

Art. 5 Änderung und Löschung von Daten durch die Ausstellerin oder Verifikatorin

Die Ausstellerin oder Verifikatorin von elektronischen Nachweisen verfügt frei über die von ihr im Basisregister eingetragenen Informationen. Sie kann über das Portal veranlassen, dass ihre eingetragenen Daten aus dem Basisregister jederzeit geändert oder gelöscht werden. Im Falle einer Löschung werden der ihr zugewiesene Identifikator, ihre kryptografischen Schlüssel und die Daten über den Widerruf einzelner Nachweise gelöscht. Die Gültigkeit bereits ausgestellter Nachweise kann in diesem Fall nicht mehr überprüft werden, da die dafür benötigten Informationen nicht mehr vorhanden sind.

Die Ausstellerin oder Verifikatorin muss nachweisen, dass sie die rechtmässige Besitzerin des Eintrages ist, insbesondere durch den Identifikator oder erforderlichen privaten kryptografischen Schlüssel. Dieser Prüfschritt erfolgt grundsätzlich automatisiert. Kann dieser Nachweis nicht mehr erbracht werden, beispielsweise aufgrund des Verlusts der privaten Schlüssel, ist eine anderweitige Glaubhaftmachung notwendig, wie

allenfalls durch die erhobenen und geprüften Daten aus dem Eintragungsprozess in das Vertrauensregister oder andere Daten zur zuverlässigen Identifizierung, wenn sie nicht im Vertrauensregister eingetragen ist. Die Bestimmung ist technologieneutral formuliert, damit aufgrund technischer Entwicklungen ein anderweitiger technischer Nachweis erbracht werden kann.

Anstatt einer Löschung des Identifikators kann die Ausstellerin oder Verifikatorin von elektronischen Nachweisen diesen deaktivieren, damit bereits ausgestellte Nachweise weiterhin verifizierbar bleiben. So können beispielsweise die von einer nicht mehr aktiven Organisation ausgestellten elektronischen Nachweise, die weiterhin gültig sind, verifiziert werden. Will sie zu einem späteren Zeitpunkt wieder einen aktiven Identifikator haben, muss sie sich erneut registrieren und im Basisregister eintragen.

Art. 6 Löschung von nicht erforderlichen Daten

Absatz 1 und 2

Stellt das BJ fest, dass eine Ausstellerin oder Verifikatorin Daten im Basisregister speichert, die für die in Artikel 2 Absatz 1 BGEID vorgesehenen Zwecke nicht erforderlich sind, beauftragt es das BIT, diese Daten oder den gesamten Eintrag zu löschen. Bevor jedoch die Daten gelöscht werden, informiert es die betroffene Ausstellerin oder Verifikatorin, sofern dies mit angemessenem Aufwand möglich ist. Stellen die eingetragenen Daten eine Cyberbedrohung dar oder enthalten sie einen rechtswidrigen Inhalt, so wird der gesamte Eintrag ohne vorgängige Informierung der betroffenen Ausstellerin oder Verifikatorin gelöscht.

Absatz 3

Beim Abfragen des Basisregisters können Daten anfallen, namentlich die IP-Adressen und andere ähnliche Daten gemäss dem benutzten Protokoll (Artikel 2 Absatz 5 Buchstabe a BGEID). Diese anfallenden Daten dürfen nur aufgezeichnet werden zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit, zur technischen Wartung der Infrastruktur oder zur Kontrolle der Einhaltung von Nutzungsreglementen (Artikel 57*l* Buchstabe b. Ziffern 1-3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[5]). Diese Aufzeichnung bezweckt den sicheren Betrieb und die sichere Funktionsweise der Vertrauensinfrastruktur sowie eine sichere Verwendung der E-ID und anderer elektronischer Nachweise. Zur Erfüllung dieses Zwecks bedarf es eine Aufbewahrung von höchstens 90 Tagen. Spätestens nach 90 Tagen müssen diese Daten vernichtet werden.

Art. 7 Aufbewahrung von geänderten oder gelöschten Daten

Gelöschte und geänderte Daten aus dem Basisregister werden vom BIT oder einer anderen Stelle des Bundes für zehn Jahre aufbewahrt, um die Nachvollziehbarkeit über

[5] SR **172.010**

die in den Registern enthaltenen Daten sicherzustellen. Die Nachvollziehbarkeit der einmal registrierten Daten ist für die Sicherstellung der Integrität, Authentizität und Beweiskraft der Daten von zentraler Bedeutung. Insbesondere muss in Rechtsstreitigkeiten nachvollzogen werden können, zu welchem Zeitpunkt welche Daten publiziert waren. Entsprechend ist die Aufbewahrung von Daten nach einer Anpassung des Eintrags im Basisregister massgeblich für die Rechtssicherheit. Die Frist von zehn Jahren entspricht dabei der allgemeinen Aufbewahrungsfrist im Geschäftsverkehr. Diese Daten sind allerdings nicht öffentlich zugänglich.

Der Bund bewahrt diese Daten auch nach Ablauf dieser zehn Jahre auf, sofern dies für die Sicherstellung einer sicheren Verwendung elektronischer Nachweise notwendig ist. Er kann in diesem Fall einzelne Daten oder den gesamten Eintrag aus dem Basisregister löschen. Diese Frist ist notwendig, damit die Rückerverfolgbarkeit, die nachträgliche Identifikation einer ehemals im Basisregister eingetragenen Ausstellerin oder Verifikatorin sowie eine sichere und vertrauensbildende Verwendung von elektronischen Nachweisen rückwirkend prüfbar bleibt.

3. Abschnitt: Vertrauensregister

Art. 8 Inhalt

Absatz 1

Das BIT stellt ein öffentlich zugängliches System zur Verfügung, das Daten für die Verifizierung der Identität von Ausstellerinnen und Verifikatorinnen und für die sichere Verwendung elektronischer Nachweise enthält (Vertrauensregister). Das Vertrauensregister ermöglicht es vom Bund geprüfte Informationen über die Identität der am System angeschlossenen Teilnehmenden abzurufen. Beispielsweise wird die Zusammengehörigkeit von Identifikator und öffentlichem Schlüssel zu fedpol bestätigt. Die Anwendung zur Vorweisung und Speicherung von elektronischen Nachweisen zeigt grundsätzlich bei einer Transaktion (Ausstellungsanfrage oder Verifikationsabfrage) Informationen aus dem Vertrauensregister dar. Am System angeschlossene Teilnehmende können jederzeit frei entscheiden, ob sie das Vertrauensregister aufrufen möchten.

Wenn ein bestätigter Identifikator im Vertrauensregister abgerufen wird, werden der im Basisregister eingetragene Identifikator und der Name oder die Firma der Ausstellerin oder Verifikatorin angezeigt, zusammen mit der Angabe, ob es sich um eine Behörde oder eine öffentliche Stelle handelt. Ist die eingetragene Ausstellerin oder Verifikatorin eine juristische Person, dann sind zudem die UID sowie allenfalls weitere Einträge in anderen Registern ersichtlich, wie z. B. ein Handelsregistereintrag. Das Vertrauensregister enthält ferner auch allfällige Informationen darüber, welche elektronischen Nachweise von Behörden oder Stellen, die öffentliche Aufgaben erfüllen, ausgestellt oder überprüft werden dürfen (Artikel 13).

Für die kryptografische Überprüfung elektronischer Nachweise oder die Erstellung von technisch sicheren Kommunikationskanälen ist das Vertrauensregister nicht erforderlich. Es soll jedoch das Vertrauen stärken, das eine Akteurin beim Gegenüber geniesst, z. B. wenn zwischen den beiden keine Beziehung besteht, wenn einer von beiden zusätzliche Informationen wünscht oder wenn eine Bestätigung der Richtigkeit der geteilten Informationen erforderlich ist. Aus diesem Grund sind im Vertrauensregister die vom Bund geprüften Informationen über die Identität einer Akteurin enthalten.

Das Vertrauensregister bietet mithin Transparenz, so dass für alle ersichtlich ist, wer beispielsweise bei der Überprüfung eines elektronischen Nachweises jeweils mehr Daten anfordert als erforderlich. Ist eine Ausstellerin oder Verifikatorin im Vertrauensregister nicht eingetragen, so ist sie durch den Bund nicht identifiziert und mithin ihre Identität nicht bestätigt. Die Daten im Vertrauensregister sind für die Öffentlichkeit zugänglich. Der Abruf der öffentlichen Daten ist ohne Registrierung möglich.

Absatz 2

Neben der Überprüfung der Identifikatoren bietet das Vertrauensregister den Nutzerinnen und Nutzern einen Vermerk bei Verdacht auf unsachgemässe Verwendung der Vertrauensinfrastruktur oder eines elektronischen Nachweises oder wenn Formate, Standards und Protokolle nach Artikel 35 nicht eingehalten werden. Dieser Hinweis soll dabei helfen, elektronische Nachweise sicher zu nutzen. Nutzerinnen und Nutzer von digitalen Brieftaschen und Check-Apps erhalten damit eine Orientierung für den sicheren Umgang.

Das Ziel ist, das Vertrauen im elektronischen Datenverkehr zu stärken und Nutzern und Nutzerinnen des Systems wirksame Indikatoren für die sichere Benutzung zu geben. Neben der Prüfung der Identität der Ausstellerinnen und Verifikatorinnen sollen die am System angeschlossenen Teilnehmenden beim Vorweisen und Verifizieren von elektronischen Nachweisen im täglichen Gebrauch das erforderliche Vertrauen haben.

Art. 9 Antrag auf Eintragung im Vertrauensregister

Absatz 1

Damit eine Behörde oder private Ausstellerin oder Verifikatorin ihren Antrag auf Eintragung ihrer Daten im Vertrauensregister stellen kann, muss sie im Basisregister eingetragen sein. Die Antragstellerin muss den erforderlichen technischen Nachweis für ihren Eintrag im Basisregister erbringen. Der zu erbringende Nachweis wird über das Portal in einem automatisierten Verfahren überprüft.

Absatz 2

Nach Artikel 3 Absatz 3 BGEID kann eine Behörde oder Stelle, die öffentliche Aufgaben wahrnimmt, einen Antrag auf Bestätigung ihres Identifikators beantragen. Mit dem Antrag sind zusätzlich zum technischen Nachweis nach Absatz 1 ihre UID und die Kontaktdaten der für den Identifikator verantwortlichen Person(en) anzugeben.

Absatz 3 und 4

Nach Artikel 3 Absatz 4 BGEID kann eine private Ausstellerin oder Verifikatorin (natürliche oder juristische Person) beantragen, dass ihr im Basisregister eingetragener Identifikator vom BIT bestätigt und im Vertrauensregister eingetragen wird.

Der Antrag einer natürlichen oder juristischen Person unterscheidet sich vom Antrag einer Behörde oder Stelle, die öffentliche Aufgaben wahrnimmt. Eine natürliche Person muss eine E-ID besitzen und diese vorweisen. Eine juristische Person muss zusätzlich zum technischen Nachweis nach Absatz 1 den Antrag auch mit einer qualifizierten elektronischen Signatur der zeichnungsberechtigten Person oder Personen im Sinne des Bundesgesetzes über die elektronische Signatur[6] vom 18. März 2016 (ZertES) versehen sowie (kumulativ) folgende Angaben machen:

- UID-Nummer;
- Kontaktdaten der juristischen Person;
- Kontaktdaten der für den Identifikator verantwortlichen Person(en); und,
- falls kein Eintrag im schweizerischen Handelsregister vorhanden ist, Belege wie eine Kopie des Gesellschaftsvertrages oder der Statuten, einen aktuellen beglaubigten Auszug aus dem ausländischen Handelsregister oder eine gleichwertige Urkunde.

Art. 10 Prüfung des Antrags

Absatz 1-2

Das BJ prüft, ob der Antrag vollständig ist und ob die eingereichten Angaben richtig sind. Sobald es den Antrag überprüft hat und die Identität der antragstellenden Person verifiziert ist beziehungsweise sichergestellt ist, dass die antragstellende Person im Namen der juristischen Person oder Personengesellschaft handeln darf, übermittelt es dem BIT das Prüfungsergebnis. Das BIT bestätigt sodann die Angaben nach Artikel 8 Absatz 1 und trägt die Bestätigung sichtbar im Vertrauensregister ein.

Absatz 3

Wenn das BJ bei der Prüfung eines Antrags feststellt, dass dieser unvollständig oder fehlerhaft ist, wird die antragstellende Person darüber informiert. Gleichzeitig wird ihr eine Frist von 30 Tagen gesetzt, um die fehlenden Angaben nachzureichen oder die Fehler zu korrigieren. Diese Regelung dient dazu, Verwaltungsverfahren effizient zu

[6] SR **943.03**

gestalten und sicherzustellen, dass für die antragstellende Person ausreichend Zeit zur Verfügung steht, etwaige Mängel zu beheben.

Wird der Antrag innerhalb dieser Frist nicht entsprechend ergänzt oder berichtigt, wird das Prüfungsverfahren eingestellt. Das bedeutet, dass der Antrag nicht weiterbearbeitet wird und kein Eintrag im Vertrauensregister erfolgt.

Art. 11 Aktualisierung

Absatz 1

Änderungen bedürfen einen neuen Antrag auf Eintragung im Vertrauensregister und müssen durch das BJ auf Vollständigkeit und Richtigkeit geprüft werden. Die Ausstellerin oder Verifikatorin meldet über das Portal (Artikel 2) jede Änderung ihrer Informationen nach Artikel 8 Absatz 1 Buchstaben b-d. Insbesondere zählen dazu: Name der natürlichen oder juristischen Person, welche im Vertrauensregister eingetragen ist; allfällige Informationen über Registereinträge der juristischen Person in anderen Registern, wie im Handelsregister, Unternehmensregister (UID-Register), Legal Entity Identifier (LEI). Die Meldung konzentriert sich dabei auf die für die Bestätigung des Identifikators erforderlichen Daten, die im Vertrauensregister veröffentlicht sind. Allfällige Änderungen an weiteren Daten, die im Rahmen des Antrags zur Eintragung bereits erhoben wurden und im Vertrauensregister nicht veröffentlicht sind, müssen nicht gemeldet werden.

Kann durch eine im Vertrauensregister eingetragene Ausstellerin oder Verifikatorin der technische Nachweis über den Besitz des ursprünglich bestätigten Identifikators erbracht werden, können ohne inhaltliche Prüfung zusätzliche Identifikatoren zum bereits bestätigten Identifikator hinzugefügt werden. In diesem Fall sind keine zusätzlichen Gebühren zu entrichten.

Absatz 2-6

Das BJ erkundigt sich bei der Ausstellerin oder Verifikatorin, ob ihre Angaben noch aktuell sind, wenn die Eintragung älter als fünf Jahre ist. Diese Erkundigung stellt keine Aufforderung dar, die aktuellen Angaben für eine erneute Prüfung durch das BJ nachzureichen (Absatz 3). Allerdings kann das Ergebnis der Erkundigung zu einem Aufforderungsverfahren führen.

Zu einem Aufforderungsverfahren kommt es, wenn das BJ Grund zur Annahme hat, dass der Eintrag nicht mehr aktuell ist und die eingetragene Ausstellerin oder Verifikatorin nicht selbst geänderte Angaben nach Absatz 1 meldet. In diesem Fall fordert es die Ausstellerin oder Verifikatorin auf, die erforderlichen Daten innerhalb von 30 Tagen zu berichtigen. Die Aufforderung muss schriftlich erfolgen, wobei diese schriftliche Aufforderung grundsätzlich elektronisch erfolgt. Sie ist kurz zu begründen und die erforderlichen Handlungen sind aufzuführen. Die Ausstellerin oder Verifikatorin muss nachvollziehen können, was und weshalb etwas von ihr gefordert wird.

Das BJ prüft die eingereichten Daten oder Belege und übermittelt dem BIT das Ergebnis seiner Prüfung zur Aktualisierung der Bestätigung. Sind die Voraussetzungen für eine Aktualisierung erfüllt, trägt das BIT diese im Vertrauensregister ein.

Für die Aufbewahrungsfristen der aus dem Vertrauensregister gelöschten Daten gilt dasselbe wie in Artikel 7 Absatz 1.

Art. 12 Löschung auf Antrag der Ausstellerin oder Verifikatorin

Absatz 1

Eine Ausstellerin oder Verifikatorin kann jederzeit die Löschung aus dem Vertrauensregister beantragen. Wird die Löschung beantragt, so wird der entsprechende Eintrag entfernt. Sofern die Löschung sich nur auf den Vertrauensregistereintrag bezieht, behält die Ausstellerin oder Verifikatorin ihren im Basisregister eingetragenen Identifikator. In diesem Fall ist bei der Verwendung elektronischer Nachweise die Identität der Ausstellerin oder Verifikatorin nicht mehr durch das BIT bestätigt. Für die Inhaberin und den Inhaber des elektronischen Nachweises ist nicht mehr bestätigt, dass die Ausstellerin oder Verifikatorin auch tatsächlich diejenige ist, für die sie sich ausgibt. Anstelle einer Löschung kann sie daher auch verlangen, dass im Vertrauensregister öffentlich zugänglich bestätigt wird, dass ein bestimmter Identifikator ihr früher zugeordnet war bzw. dass ihr Identifikator bis zur Deaktivierung bestätigt war.

Wie beim Löschungsantrag bezüglich eines Basisregistereintrags muss die im Vertrauensregister eingetragene Ausstellerin oder Verifikatorin nachweisen, dass sie die rechtmässige Besitzerin des Eintrages ist, insbesondere durch den Identifikator oder erforderlichen privaten kryptografischen Schlüssel (vgl. Artikel 5). Zusätzlich wird vom BJ geprüft, ob die antragstellende Behörde, Stelle oder Person über den erforderlichen Identitätsnachweis verfügt.

Absatz 2

Wurde eine Ausstellerin oder Verifikatorin nach Artikel 11 Absatz 3 vom BJ aufgefordert, Belege für die Aktualisierung ihres Eintrags vorzulegen, und kommt sie der Aufforderung nicht fristgerecht nach, veranlasst das BJ beim BIT die Löschung der Bestätigung ihres Identifikators aus dem Vertrauensregister.

Absatz 3

Die Aufbewahrungsfrist für den gelöschten bestätigten Identifikator aus dem Vertrauensregister richtet sich nach Artikel 7 Absatz 1. Die Aufbewahrungsfrist gilt auch für allfällige Änderungen an den Vertrauensregisterdaten (geprüfte Mutationen von Einträgen im Vertrauensregister). Demnach gilt ebenfalls grundsätzlich eine zehnjährige Aufbewahrungsfrist und, sofern es für die sichere Verwendung elektronischer Nachweise erforderlich ist, kann der Bund die Daten auch über diese zehnjährige Frist hinaus aufbewahren.

Art. 13 Eintragung anderer Daten durch Behörden

Neben dem bestätigten Identifikator und dem Vermerk eines Verdachts auf unsachgemässe Verwendung der Vertrauensinfrastruktur oder eines elektronischen Nachweises nach Artikel 18 stellt das Vertrauensregister den Nutzerinnen und Nutzern auch Informationen zur Verfügung, die von einer Behörde oder Stelle, die öffentliche Aufgaben wahrnimmt, bereitgestellt worden sind. Darunter fallen insbesondere Daten, anhand deren festgestellt werden kann, welche Behörde oder öffentliche Stelle eine bestimmte Art von elektronischem Nachweis ausstellen und überprüfen darf. Die Behörde oder Stelle, die diese Informationen zur Verfügung stellt, ist für deren Richtigkeit verantwortlich.

Die Behörden und andere Stellen, die öffentliche Aufgaben erfüllen, müssen im Basis- und Vertrauensregister eingetragen sein, damit sie zusätzliche Daten selbst in das Vertrauensregister eintragen können. Ihnen wird auf Antrag beim BJ ein dedizierter Zugang zum System gewährt. Sie können dadurch eigenständig Informationen über die von ihnen verantworteten Typen von Nachweisen publizieren. Dazu gehören beispielsweise technische Schemata, welche festlegen, aus welchen Datenfeldern ein Nachweis besteht. Zudem kann hinterlegt werden, welche Akteure anhand ihrer Identifikatoren als legitime Austellerinnen und Verifikatorinnen gelten. Mindestens einzutragen sind dabei der Identifikator oder die Identifikatoren der betroffenen Behörde(n) oder Stelle(n) und die Bezeichnung des jeweiligen elektronischen Nachweises.

4. Abschnitt: Digitale Anwendungen

Art. 14 Anforderungen an die Anwendung zur Aufbewahrung und Vorweisung elektronischer Nachweise

Absatz 1

Das BIT stellt eine Software-Anwendung zur Aufbewahrung und Vorweisung der elektronischen Nachweise (staatliche elektronische Brieftasche) zur Verfügung. Es muss dabei sicherstellen, dass die Anwendung für Menschen mit Behinderungen zugänglich ist (Artikel 28 Absatz 2 BGEID). Damit eine sichere Funktionsweise der Anwendung sichergestellt werden kann, muss eine Nutzerin oder ein Nutzer ein Endgerät verwenden, das gewisse Anforderungen erfüllt. Diese Anforderungen orientieren sich an aktuellen, verbreiteten Branchenstandards bei der Entwicklung von mobilen Anwendungen. Hierzu gehört, dass das auf dem Endgerät installierte Betriebssystem eine weite Verbreitung kennt, nach wie vor von der jeweiligen Systemanbieterin unterstützt wird und weiterhin Sicherheitsupdates erhält.

Absatz 2

Ist eine Ausstellerin nicht im Basisregister oder Vertrauensregister eingetragen (Buchstabe a) oder ist eine Verifikatorin nicht im Basisregister oder Vertrauensregister eingetragen und verwendet sie nicht die vom Bund zur Verfügung gestellte Anwendung

zur Überprüfung elektronischer Nachweise (Buchstabe b), so ist für eine Nutzerin oder einen Nutzer unter Umständen nicht ersichtlich, mit wem sie interagiert. Diese fehlende Registrierung stellt ein erhöhtes Risiko für den Datenschutz dar, da die Identität der beteiligten Parteien nicht eindeutig nachvollzogen werden kann. Ohne diese Transparenz wird es schwierig, die Vertrauenswürdigkeit der Akteurinnen und Akteure zu prüfen. Es können zudem auch keine Sicherheitsinformationen vermerkt werden, was potenziell zu Missbrauch, unbefugtem Zugriff auf personenbezogene Daten oder anderen Sicherheitslücken führen kann.

Als angemessene technische und organisatorische Massnahme zum Schutz und zur Sicherheit im elektronischen Datenverkehr (Artikel 33 Buchstabe e BGEID) zeigt die Anwendung der Nutzerin oder dem Nutzer vor einer möglichen Datenübertragung daher jeweils an, wenn eine Ausstellerin oder Verifikatorin nicht im Basisregister oder Vertrauensregister eingetragen ist. Verwendet eine Verifikatorin aber die Anwendung des Bundes zur Überprüfung elektronischer Nachweise, so entfällt diese Anzeige und der Nutzerin oder dem Nutzer wird dargestellt, dass die Verifikatorin die offizielle Anwendung zur Prüfung elektronischer Nachweise des Bundes nach Artikel 9 BGEID verwendet. In diesem Fall wird der Nutzerin oder dem Nutzer durch datenschutzfreundliche Vorsteinstellung der Anwendung zur Überprüfung gewährleistet, dass eine sichere Datenübertragung stattfindet.

Art. 15 System für Sicherheitskopien

Nach dem Verlust oder Kauf eines neuen Endgeräts (z. B. Smartphone) ist im Allgemeinen üblich, dass installierte Anwendungen und gespeicherte Daten aus einem Backup wiederhergestellt werden. So können die Funktionalitäten des alten Systems bei einem Wechsel des Endgeräts rasch wieder verfügbar gemacht werden. Eine vergleichbare Möglichkeit wird den Inhaberinnen und Inhabern der staatlichen elektronischen Brieftasche angeboten. Die wiederverwendbare Wiederherstellung von elektronischen Nachweisen ist nicht möglich, wenn wie bei der E-ID eine Bindung mittels Krypto-Prozessor an das mobile Endgerät der Inhaberin oder den Inhaber erforderlich ist. Entsprechend müssen solche elektronischen Nachweise bei der Ausstellerin neu beantragt werden.

Absatz 1

Als Basisfunktion in der Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen ist vorgesehen, dass durch die Inhaberinnen und Inhaber eine Sicherungskopie des Inhalts (insb. die elektronischen Nachweise) der elektronischen Brieftasche generiert und verschlüsselt werden kann. Die Inhaberinnen und Inhaber können selbst entscheiden, wo sie diese Sicherungskopie aufbewahren wollen. Nach einem Wechsel des Endgerätes (Smartphone, Computer usw.) können die gespeicherten elektronischen Nachweise manuell wiederhergestellt werden.

Die Übertragung und Wiederherstellung dieser Sicherungskopien werden massgeblich durch die Funktionen beeinflusst, die vom Betriebssystem des Endgeräts zur Verfügung gestellt werden. Zudem müssen sich Inhaberinnen an ein Passwort (Bsp. Wordlist-Verschlüsselung) erinnern, welches notwendig ist, um die erstellten Sicherheitskopien zu entschlüsseln. Im Falle des Verlustes oder Vergessens dieses Passworts ist eine Wiederherstellung der Daten nicht möglich. Die Passwörter sind dem Bund nicht bekannt.

Absatz 2

Das BIT stellt ein Informatiksystem bereit, in welchem die Inhaberinnen und Inhaber die auf ihrem Endgerät erstellten Sicherheitskopien speichern können (Artikel 8 Absatz 2 BGEID). Das System ist so ausgestaltet, dass Dritte nicht darauf zugreifen können. Die Nutzung des Systems für Sicherheitskopien ist freiwillig und nur für Nutzerinnen und Nutzer der staatlichen elektronischen Brieftasche möglich. Nur die Inhaberinnen und Inhaber können auf den Inhalt ihrer Sicherheitskopien zugreifen. Bei längerer Inaktivität, wenn die Sicherheitskopien nicht aktualisiert oder heruntergeladen werden, werden die Dateien nach drei Jahren gelöscht.

Es gilt zu berücksichtigen, dass Nachweise nach dem Einlesen der Daten aus einem Backup nicht mehr gültig verwendet werden können, wenn wie bei der E-ID eine Bindung mittels eines Krypto-Prozessors an die Inhaberin oder den Inhaber vorgesehen wird (vgl. Artikel 18 Absatz 2 BGEID). Der Nachweis der Inhaberbindung ist in diesem Fall an das ursprünglich bei der Ausstellung verwendete Endgerät gebunden. Bei einem Verlust oder Wechsel des entsprechenden Endgeräts ist deshalb für die Nutzung der entsprechenden Nachweise eine Neuausstellung erforderlich.

Art. 16 Prüfung anderer elektronischer Nachweise mithilfe der Anwendung nach Artikel 9 BGEID

Absatz 1 und 2

Diese Bestimmung konkretisiert die Delegationsnorm nach Artikel 9 Absatz 2 BGEID für die Prüfung anderer elektronischer Nachweise durch die Bundes-Check-App. Neben der in Absatz 1 geregelten Prüfung der E-ID soll die Bundes-Check-App auch die Gültigkeit weiterer elektronischer Nachweise prüfen können. Ziel ist es, die Nutzung der Vertrauensinfrastruktur und die Verbreitung elektronischer Nachweise zu fördern.

Die Verwendung der Bundes-Check-App für die Überprüfung elektronischer Nachweise ist freiwillig. Verifikatorinnen können frei wählen, ob sie die Anwendung des Bundes oder eine andere, gleichwertige Lösung verwenden möchten.

Behörden, Organisationen mit öffentlichen Aufgaben sowie private Ausstellerinnen können beim BJ beantragen, dass ihre elektronischen Nachweise über die Bundes-Check-App überprüfbar sind. Voraussetzung ist, dass die Nachweise den technischen Anforderungen (Formate, Standards und Protokolle) entsprechen und die Ausstellerin im Vertrauensregister eingetragen ist.

Absatz 3

Damit ein elektronischer Nachweis einer privaten Ausstellerin über die Bundes-Check-App geprüft werden kann, muss zusätzlich zu den Anforderungen nach Absatz 2 gewährleistet sein, dass keine öffentlichen Interessen – insbesondere im Hinblick auf Sicherheit oder Datenschutz – entgegenstehen. Zudem ist erforderlich, dass der Nachweis in der Praxis breit genutzt und allgemein anerkannt ist.

Die Bundes-Check-App ist primär für die Überprüfung der E-ID vorgesehen. Ihre Erweiterung auf weitere elektronische Nachweise erfordert zusätzlichen technischen und organisatorischen Aufwand sowie entsprechende Ressourcen. Um sicherzustellen, dass diese Erweiterungen den öffentlichen Interessen dienen und in Bezug auf den Aufwand verhältnismässig bleiben, sollen über die Anwendung des Bundes Nachweise von übergeordneter gesellschaftlicher Relevanz überprüft werden können.

Absatz 4

Wenn eine Ausstellerin möchte, dass die Check-App ihre elektronischen Nachweise überprüft, kann sie beim BJ einen Antrag stellen. Die Anpassung der Check-App ist eine kostenlose Dienstleistung. Erfüllt ein elektronischer Nachweis der antragstellenden Ausstellerin alle Anforderungen, um in die Check-App des Bundes aufgenommen zu werden, so trifft das BJ den Entscheid zur Erweiterung der Anwendung und es meldet dem BIT, die erforderlichen Massnahmen zu ergreifen.

5. Abschnitt: Unsachgemässe Verwendung von Vertrauensinfrastruktur und elektronischen Nachweisen

Art. 17 Prüfverfahren

Absatz 1 und 2

Erhält das BJ Kenntnis von einer unsachgemässen Verwendung der Vertrauensinfrastruktur oder eines elektronischen Nachweises, z. B. durch eine Inhaberin oder einen Inhaber eines elektronischen Nachweises, oder von einer Ausstellerin oder Verifikatorin, so führt es ein Prüfverfahren durch. Diese Prüfung dient dem Schutz der Wahrung der Integrität des Systems, in dem die elektronischen Nachweise verwendet werden. Den am System Angeschlossenen steht die Möglichkeit zur Meldung zur Verfügung, die sicherstellt, dass Sicherheitsmängel schnell erkannt und adressiert werden können, um Risiken für die Sicherheit und den Datenschutz zu minimieren. Der Verordnungsentwurf präzisiert, wann eine unsachgemässe Verwendung vorliegt:

a. Als wichtige Voraussetzung für eine sichere Verwendung elektronischer Nachweise muss eine Ausstellerin oder Verifikatorin ihre offiziellen Angaben nutzen. Sie verwendet beispielsweise keine offiziellen Angaben, wenn die im Vertrauensregister eingetragene Identität einer Person nicht mit der tatsächlichen Identität übereinstimmt, oder wenn sie sich im Geschäftsverkehr als eine Person

ausgibt, die sie nicht ist. Letzteres gilt auch für eine Ausstellerin oder Verifikatorin, die ausschliesslich im Basisregister eingetragen ist.

Die offizielle Identität kann bei natürlichen Personen, analog zum Inhalt der E-ID nach Artikel 15 Absatz 3 BGEID, auch zusätzliche Daten umfassen, wie z. B. den Allianz-, Ordens-, Künstler- oder Partnerschaftsnamen und die Angabe von besonderen Kennzeichen. Solche Angaben können in gewissen Fällen für Transaktionen im Geschäftsverkehr nützlich oder sogar erforderlich sein. Sie können daher Teil der Identität darstellen, wenn sie auch im Ausweis, in einem anderen Ausweispapier oder in der Legitimationskarte der Inhaberin oder des Inhabers angegeben sind und im Antragsverfahren nach Artikel 9 verwendet wurden. Letzteres trifft sodann auch auf juristische Personen zu, deren Identität insbesondere durch ein bestimmtes Markenprodukt oder eine bestimmte Dienstleistung bekannt sein kann.

b. Ein Nachweis darf keine rechtswidrigen Inhalte enthalten oder einem rechtswidrigen Zweck dienen.

c. Wenn ein elektronischer Nachweis besonders schützenswerte personenbezogene Daten enthält, wie etwa Gesundheitsdaten oder Informationen über die religiöse Überzeugung, muss die Inhaberin oder der Inhaber dieses Nachweises schriftlich darüber informiert werden. Diese Information soll klarstellen, dass die enthaltenen Daten besonders sensibel sind und daher einem höheren Schutz unterliegen. Auf diese Weise wird sichergestellt, dass die betroffene Person sich der Sensibilität ihrer Daten bewusst ist und gegebenenfalls ihre Zustimmung zur Verarbeitung erteilen kann. Die schriftliche Mitteilung dient also dem Zweck, die Inhaberin oder den Inhaber über die Bedeutung und den Schutz dieser Daten aufzuklären, bevor eine spezifische Verarbeitung erfolgt. Die elektronische Brieftasche des Bundes unterstützt ein Datenformat, welches es Ausstellerinnen erlaubt, sensitive Informationen direkt in der Applikation zu kennzeichnen. Nutzende werden bei der Anfrage eines entsprechenden Datenfelds explizit vor der Übermittlung darüber gewarnt.

d. Für eine sichere Verwendung elektronischer Nachweise sind beim Überprüfen eines elektronischen Nachweises die grundlegenden Prinzipien des Datenschutzes zu wahren. Das bedeutet insbesondere, dass die personenbezogenen Daten nicht in einem unverhältnismässigen Umfang erhoben werden dürfen. Die Daten dürfen sodann nur für den klar definierten und für die betroffene Person erkennbaren Zweck erhoben werden. Das heisst, eine Nutzung der Daten für andere, nicht im Vorfeld festgelegte Ziele ist unzulässig. Sobald die Daten nicht mehr für den verfolgten Zweck benötigt werden, müssen diese entweder vernichtet oder anonymisiert werden. Diese Vorgehensweise schützt die Privatsphäre der betroffenen Personen und gewährleistet, dass die Verarbeitung ihrer Daten stets im Einklang mit den Datenschutzbestimmungen erfolgt.

Absatz 3 und 4

Für die Prüfung eines Verdachts kann das BJ verschiedene Massnahmen ergreifen. Es kann beispielsweise die über das Portal zur Bearbeitung von Registerdaten nach Artikel 2 erfassten Daten sowie die Daten aus dem Basisregister und Vertrauensregister prüfen. Des Weiteren kann es zum Beispiel bereits bei der Meldung technische Angaben zu den übermittelten Daten erhalten oder diese nachgelagert anfordern, um sicherzustellen, dass diese korrekt und sicher verarbeitet wurden. Zudem kann das Amt Nachforschungen zur Herkunft des elektronischen Nachweises anstellen, um etwaige Sicherheitslücken oder Unregelmässigkeiten aufzudecken. Darüber hinaus hat es die Möglichkeit, direkten Kontakt mit der betroffenen Inhaberin oder dem betroffenen Inhaber des Nachweises sowie mit der Ausstellerin oder Verifikatorin des in Frage stehenden elektronischen Nachweises aufzunehmen. In diesem Rahmen kann das BJ weitere Informationen zur betreffenden Transaktion verlangen, um den Sachverhalt zu klären.

Das BJ kann eine unsachgemässe Verwendung nur prüfen, wenn ein eindeutiger Identifikator verwendet wird. Bei einem Verdacht auf schwerwiegende Datenschutzverletzungen informiert das BJ den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten oder die zuständige kantonale Stelle über die betreffende unsachgemässe Verwendung.

Art. 18 Vermerk betreffend unsachgemässe Verwendung

Stellt das BJ nach einer Prüfung nach Artikel 17 Absatz 3 fest, dass eine unsachgemässe Verwendung der Vertrauensinfrastruktur oder elektronischer Nachweise vorliegt, so meldet es das Ergebnis der Prüfung dem BIT. Das BIT trägt das Ergebnis im Vertrauensregister für höchstens sechs Monate sichtbar ein. Das BJ informiert zugleich die betroffene Ausstellerin oder Verifikatorin, sofern dies mit angemessenem Aufwand möglich ist. Der Eintrag dient dabei der Transparenz und Vertrauensbildung, sodass die Nutzerinnen und Nutzer informiert entscheiden können, ob sie den elektronischen Nachweis in einem bestimmten Kontext verwenden möchten. Dies trägt dazu bei, die gesamte Sicherheit im System der elektronischen Nachweise zu erhöhen und die Richtigkeit der Informationen im Vertrauensregister sicherzustellen. Die Sichtbarkeit eines Vermerks wird spätestens nach Ablauf der nach Absatz 3 festgelegten Frist aus dem Vertrauensregister gelöscht.

Die Sichtbarkeit eines Vermerks kann verlängert werden. Das BJ prüft nach Ablauf der Frist oder sofern neue Meldungen eingehen, ob eine unsachgemässe Verwendung weiterhin vorliegt. Sollte dies der Fall sein, wird der Eintrag für einen weiteren Zeitraum sichtbar gehalten, um weiterhin die sichere Verwendung elektronischer Nachweise zu ermöglichen. Diese Verlängerung in offensichtlichen Fällen stellt sicher, dass die Nutzerinnen und Nutzer über aktuelle Informationen zur unsachgemässen Verwendung der Vertrauensinfrastruktur oder eines elektronischen Nachweises verfügen und somit informierte Entscheidungen treffen können, ohne dass zwingend eine Meldung zu erfolgen hat. Die Transparenz und Vertrauensbildung trägt dazu bei, dass kontinuierlich die erforderlichen rechtlichen Vorgaben eingehalten werden, um das Vertrauen in Vertrauensinfrastruktur und die elektronische Nutzung von Nachweisen aufrechtzuerhalten.

Eine offensichtliche anhaltende unsachgemässe Verwendung liegt beispielsweise vor, wenn eine Ausstellerin oder Verifikatorin sich als eine Person ausgibt, die sie nicht ist, wenn eine Ausstellerin elektronische Nachweise mit rechtswidrigen Inhalten oder zu rechtswidrigen Zwecken ausstellt oder eine Ausstellerin oder Verifikatorin als automatisiertes Programm (BOT) identifiziert wurde. Bei einer Verlängerung aus offensichtlichen Gründen kann das BJ vorsehen, dass die Eintragung unbefristet publiziert wird.

Art. 19 Löschung des Vermerks

Das BIT löscht den Vermerk nach Ablauf der festgelegten Dauer aus dem Vertrauensregister. Die mit dem Vermerk zusammenhängenden Daten, wie auch die im Rahmen des Prüfverfahrens durch das BJ erfassten Informationen, werden vom Bund zehn Jahre aufbewahrt und sind nicht öffentlich zugänglich. Der Bund kann die gelöschte Eintragung auch nach zehn Jahren noch aufbewahren, wenn dies für die sichere Verwendung der Vertrauensinfrastruktur oder der elektronischen Nachweise erforderlich ist.

3. Kapitel: E-ID

1. Abschnitt: Antrag

Art. 20 Allgemeine Voraussetzungen

Absatz 1

Wer eine E-ID erhalten möchte, muss ein Endgerät verwenden, das die Bindung nach Artikel 18 Absatz 2 BGEID sicherstellt, sowie auf dem Endgerät eine Anwendung nach Artikel 8 Absatz 1 BGEID oder eine andere Anwendung nach Artikel 18 Absatz 4 oder 5 BGEID installieren, in die die E-ID ausgestellt wird. Die Inhaberin oder der Inhaber des Endgeräts kann in der Anwendung sowohl die eigene E-ID als auch die einer anderen Person aufbewahren, etwa die einer minderjährigen Person oder einer Person unter umfassender Beistandschaft, sofern sie oder er deren gesetzliche Vertretung innehat.

Artikel 18 Absatz 4 BGEID erweitert die Möglichkeiten, auch andere Lösungen für die Sicherstellung einer Bindung an die Inhaberin oder den Inhaber sicherzustellen. Die Bestimmung ist bewusst technologieneutral formuliert, damit verschiedene Lösungen in Frage kommen. Grundsätzlich bedarf es aber einer automatisierten Sicherstellung sowie eines technischen Nachweises, welcher beispielsweise darlegt, dass das für die Inhaberbindung verwendete kryptografische Schlüsselpaar von einem dedizierten Hardware-Krypto-Prozessor stammt.

Absatz 2 und 3

Der Antrag muss von der zukünftigen Inhaberin oder vom zukünftigen Inhaber der E-ID gestellt werden. Ist die betreffende Person minderjährig oder unter umfassender

Beistandschaft, muss sie die Genehmigung ihrer gesetzlichen Vertretung vorlegen. Diese kann ihre Zustimmung direkt im Online-Verfahren mit ihrer eigenen E-ID erteilen, sofern sie über eine solche verfügt. Ist dies nicht der Fall, muss sie die unterschriebene Einwilligung der minderjährigen oder unter umfassender Beistandschaft stehenden Person aushändigen oder sie begleiten, wenn diese ihre Identität bei einem Erfassungszentrum, einer Migrationsbehörde oder einer Schweizer Vertretung im Ausland überprüfen lässt. Bei minderjährigen Antragsstellerinnen und Antragstellern mit gemeinsamer elterlicher Sorge reicht die Einwilligung eines Elternteils aus.

Art. 21 Anforderungen an das Gesichtsbild

Die Identitätsprüfung anhand einer automatisierten Gesichtsüberprüfung kann nur durchgeführt werden, wenn in den Informationssystemen nach Artikel 17 Absatz 2 BGEID ein Lichtbild des Antragstellers vorhanden ist. Darüber hinaus muss dieses Foto von ausreichender Qualität sein und den Standards des Abkommens vom 7. Dezember 1944 über die internationale Zivilluftfahrt (ICAO)[7] entsprechen. Ausserdem muss es elektronisch gespeichert und abrufbar sein.

Art. 22 Einreichung des Antrags

Die Antragstellerin oder der Antragsteller muss den Antrag über die Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen nach Artikel 8 BGEID (elektronische Brieftasche des Bundes) einreichen.

Art. 23 Identitätsprüfung mithilfe der Anwendung nach Artikel 8 BGEID

Absatz 1

Die Antragstellerin oder der Antragsteller kann seine Identität über die Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen überprüfen lassen, wenn ihre oder seine Identität mindestens einmal vor Ort überprüft wurde. Das heisst, dass die Identitätsprüfung entweder bei der erstmaligen Ausstellung der E-ID oder im Rahmen der Ausstellung des Dokuments nach Artikel 14 Buchstabe a BGEID (Identitätsausweis, Reisepass, Ausländerausweis oder Legitimationskarte) einmal vor Ort erfolgt sein muss.

Verfügt die Antragstellerin oder der Antragsteller über einen gültigen Ausweis im Sinne von Artikel 17 Absatz 1 der Gaststaatverordnung vom 7. Dezember 2007[8] in Verbindung mit Artikel 71*a* Absatz 1 der Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE) erfolgt die Identitätsprüfung vor Ort bei einer vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) bezeichneten Passstelle oder Migrationsbehörde.

[7] SR **0.748.0**

[8] SR **192.121**

Absatz 2

Um ihre oder seine Identität online zu überprüfen, scannt die Antragstellerin oder der Antragsteller den maschinenlesbaren Bereich (MRZ) oder den CHIP ihres oder seines amtlichen Ausweises (Identitätsausweis, Reisepass oder Ausländerausweis) und filmt anschliessend sein Gesicht (Liveness-Check). Sie oder er übermittelt das Ergebnis des Scans und/oder der CHIP-Auslesung sowie ihr oder sein Gesichtsbild (in Form von Videoausschnitten) direkt über die Anwendung an das fedpol, das den Antrag prüft.

Absatz 3

Zur Überprüfung der von der Antragstellerin oder vom Antragsteller übermittelten Daten nutzt fedpol einen Teil des Informationssystems zur Ausstellung und zum Widerruf der E-ID nach Artikel 26 Absatz 1 BGEID. Dieses System ermöglicht einen automatisierten Abgleich der übermittelten Informationen – insbesondere des Gesichtsbildes – mit den Informationen in den Informationssystemen, auf die fedpol gemäss Artikel 26 Absatz 3 BGEID Zugriff hat. Das fedpol kann zum Zwecke der Qualitätskontrolle in den Abgleich von Gesichtsbildern eingreifen.

Art. 24 Identitätsprüfung vor Ort

Antragstellende, die anstelle der Identitätsprüfung über die Anwendung zur Aufbewahrung und Vorweisung elektronischer Nachweise eine persönliche Identitätsprüfung vor Ort wünschen, müssen hierfür einen Termin vereinbaren. Für die vor Ort erbrachten Leistungen können Gebühren erhoben werden.

Die zuständige kantonale Behörde bzw. die Schweizer Vertretung im Ausland überprüft die Identität der antragstellenden Person anhand des von ihr vorgelegten Ausweises, ihres Gesichts und der Informationen aus den Informationssystemen nach Artikel 17 Absatz 2 BGEID. Der Gesichtsabgleich kann automatisch erfolgen. Zu diesem Zweck kann die Station zur Erfassung biometrischer Daten verwendet werden (maschinelle Prüfung). In diesem Fall ist die Antragstellerin oder der Antragsteller darüber zu informieren, dass ihre oder seine Identität mit Hilfe der Erfassungsstation überprüft wird. Dieses Gerät bietet eine Entscheidungshilfe in Form einer Bewertung, die endgültige Entscheidung liegt jedoch bei der Fachperson. Bei der Identitätsprüfung vor Ort werden keine Daten im System gespeichert oder aufbewahrt. Das Ergebnis der Identitätsprüfung wird in elektronischer Form über das Informationssystem zur Ausstellung und zum Widerruf der E-ID an das fedpol übermittelt.

Wer eine E-ID ausgestellt erhalten möchte, kann dies zusammen mit einem Antrag auf eine Identitätskarte oder einen Reisepass nach Artikel 14 Buchstabe a Ziffer 1 BGEID (Variante *Ausweis+*) tun. Bei einem gemeinsamen Antrag erfolgt die Identitätsprüfung im Rahmen der Ausstellung des oder der Ausweise nach Artikel 14 Buchstabe a Ziffer 1 BGEID. Die Möglichkeit, eine E-ID gleichzeitig mit einem Pass und/oder einer Identitätskarte zu beantragen, ist eine zusätzliche Dienstleistung. Da die Identitätsprüfung bereits erfolgt ist, ist bei einem Antrag auf gemeinsame Ausstellung keine zusätzliche

Identitätsprüfung zur Validierung der Ausstellung der E-ID vorgesehen. Nach Abschluss des Identitätsprüfungsverfahrens kann die Ausstellung der E-ID vor Erhalt des Ausweises erfolgen.

Auslandschweizerinnen und -schweizer gemäss dem Bundesgesetz über Schweizer Personen und Institutionen im Ausland[9] vom 26. September 2014 (ASG) können ihre Identität bei der zuständigen konsularischen Vertretung der Schweiz überprüfen lassen.

Art. 25 Automatisierte Entscheidung

Bei der Installation der Anwendung wird die Antragstellerin oder der Antragsteller nach Artikel 21 des Datenschutzgesetzes[10] vom 25. September 2020 (DSG), über die automatisierte Verarbeitung ihrer oder seiner personenbezogenen Daten informiert. Um den Vorgang fortzusetzen, muss sie oder er ausdrücklich der automatisierten Entscheidung zustimmen. Auf Antrag beim technischen Supportdienst von fedpol oder aus Gründen der Qualitätskontrolle kann die automatisierte Entscheidung von einer mit der Identitätsprüfung beauftragten Fachperson überprüft werden.

Artikel 21 Absatz 1 DSG sieht vor, dass die für die Datenbearbeitung verantwortliche Person die betroffene Antragstellerin oder den betroffenen Antragsteller über jede Entscheidung informiert, die ausschliesslich auf der Grundlage einer automatisierten Bearbeitung personenbezogener Daten getroffen wird und die ihr oder ihm gegenüber rechtliche Wirkung entfaltet oder sie oder ihn erheblich beeinträchtigt (automatisierte Einzelentscheidung). Artikel 21 Absatz 2 DSG ergänzt, dass die für die Bearbeitung verantwortliche Person auf Antrag der antragstellenden Person die Möglichkeit geben muss, ihren Standpunkt darzulegen.

Art. 26 Beantragung der E-ID im Ausland

Kann die Anwendung nach Artikel 8 Absatz 1 BGEID oder die Anwendung nach Artikel 18 Absatz 4 oder 5 BGEID im Ausland nicht installiert werden, insbesondere aufgrund geografischer Sperrung, so kann die E-ID nicht beantragt werden.

2. Abschnitt: Ausstellung und Widerruf

Die E-ID wird ausschliesslich von fedpol für natürliche Personen über die staatliche Vertrauensinfrastruktur in Form eines elektronischen Identitätsnachweises ausgestellt. Mit der E-ID kann man sich in der virtuellen Welt identifizieren, was für bestimmte Online-Vorgänge erforderlich ist, beispielsweise um einen Strafregisterauszug zu beantragen oder bei einem zertifizierten Anbieter eine elektronische Signatur zu erhalten,

[9] SR **195.1**

[10] SR **235.1**

mit der man rechtsgültig unterschreiben kann. Sie ist vergleichbar mit dem Identitätsausweis oder dem Reisepass in der physischen Welt. Die E-ID ersetzt jedoch nicht diese beiden Dokumente. Alle Bürgerinnen und Bürger müssen frei entscheiden können, ob sie eine E-ID, eine physische Identitätskarte oder einen Pass verwenden möchten.

In den meisten Fällen kann fedpol die für die Ausstellung der E-ID erforderlichen Aufgaben automatisiert ausführen. Bestehen Zweifel bei fedpol oder Unsicherheiten im automatischen System, kann fedpol eingreifen und die bei der Gesichtsüberprüfung generierten Daten überprüfen. fedpol entscheidet, wann die automatisierte Entscheidung von einer Kontrollinstanz überprüft werden muss.

Art. 27 Ausstellung

Absatz 1

Für denselben Antrag kann die E-ID in mehrere Anwendungen auf einem oder mehreren Endgeräten (höchstens bis zu zehn elektronischen Brieftaschen) ausgestellt werden. Die gleichzeitige Ausstellung soll einen Missbrauch der E-ID verhindern.

Absatz 2

Die folgenden Daten über den Ausstellungsprozess werden im Informationssystem zur Ausstellung und zum Widerruf der E-ID gespeichert:

a. Werte der automatischen Identitätsprüfungen mithilfe der Anwendung nach Artikel 8 BGEID;

b. die Identifikationsnummer der Person, die die Identitätsprüfung vornimmt und die von ihr getroffenen Entscheidungen;

c. Vorname, Nachname und E-ID-Nummer der gesetzlichen Vertretung;

d. Informationen über die Bindung der E-ID an die Inhaberin oder den Inhaber;

e. Versionsnummern der Teile oder des gesamten Informationssystems zur Ausstellung und zum Widerruf der E-ID;

f. Beginn- und Enddatum des Ausstellungsprozesses;

g. technischer Kennwert der E-ID (z. B. ein aus kryptografischem Hashing resultierender Code oder Hashwert).

Diese Daten, einschliesslich der biometrischen Daten nach Artikel 17 Absatz 4 BGEID, die zur Untersuchung einer Erschleichung oder missbräuchlichen Verwendung einer E-ID erforderlich sind und ausschliesslich zu diesem Zweck aufbewahrt werden, werden gemäss Artikel 27 Absatz 1 Buchstabe b BGEID fünf Jahre nach Ablauf der Gültigkeit der E-ID vernichtet.

Absatz 3

In der Departementsverordnung werden insbesondere das technische Format und die Attribute zur Übermittlung von Daten, die Anforderungen an die Schnittstelle mit dem Informationssystem zur Ausstellung und zum Widerruf der E-ID sowie die Standards und Protokolle für die Datenbekanntgabe bei der Ausstellung der E-ID geregelt. Zurzeit sind die Anforderungen noch in Entwicklung und auf GitHub dokumentiert.

Art. 28 Gültigkeitsdauer

Absatz 1 und 2

Die Gültigkeitsdauer der E-ID richtet sich nach dem Ausstellungsdatum: Sie ist ab dem Zeitpunkt gültig, an dem sie von fedpol ausgestellt wird. Wurden im Rahmen desselben Antrags mehrere E-ID ausgestellt, gilt das Ausstellungsdatum der zuerst ausgestellten E-ID.

Bei einem Antrag auf gemeinsame Ausstellung zusammen mit einem der in Artikel 14 Buchstabe a Ziffer 1 BGEID genannten Ausweise beginnt die Gültigkeitsdauer der E-ID ab dem Ausstellungsdatum der E-ID und nicht ab dem Ausstellungsdatum des jeweiligen Ausweises oder der Ausweise.

Die E-ID ist höchstens so lange gültig wie das Dokument, das während des Antrags verwendet wurde.

Absatz 3

Aus Gründen der Informationssicherheit kann das EJPD eine kürzere Gültigkeitsdauer festlegen. Die Gültigkeitsdauer der E-ID darf die Gültigkeitsdauer des im Rahmen des Ausstellungsverfahrens verwendeten Dokuments nicht überschreiten.

Art. 29 Antrag auf Widerruf

Absatz 1

Auf Antrag der Inhaberin oder des Inhabers oder, im Fall einer minderjährigen Person oder einer Person unter umfassender Beistandschaft, auf Antrag ihrer oder seiner gesetzlichen Vertretung kann fedpol die E-ID widerrufen. Eine minderjährige Person oder eine Person unter umfassender Beistandschaft kann den Widerruf ihrer eigenen E-ID ohne die Zustimmung ihrer gesetzlichen Vertretung beantragen.

Absatz 2 und 3

Für jeden Widerrufsantrag bei fedpol muss die Inhaberin oder der Inhaber der E-ID oder die gesetzliche Vertretung einer minderjährigen Person oder einer Person unter umfassender Beistandschaft ihre oder seine Identität mit einem gültigen Identitätsdokument nachweisen oder, sofern sie oder er (noch) im Besitz der E-ID ist, mit dieser.

Wenn der Antrag von der gesetzlichen Vertretung gestellt wird, muss diese zusätzlich die Identität der minderjährigen Person oder der Person unter umfassender Beistandschaft sowie ihre Vertretungsberechtigung nachweisen.

Absatz 4

Bei Verlust des Endgeräts kann die Inhaberin oder der Inhaber beziehungsweise die gesetzliche Vertretung den Verlust einer Polizeibehörde oder einer konsularischen Vertretung melden. Diese informiert fedpol, welches die E-ID daraufhin unverzüglich widerruft.

Art. 30 Verfahren bei Verdacht auf Erschleichung oder missbräuchliche Verwendung oder auf Gefährdung der Sicherheit

Besteht der Verdacht auf Erschleichung oder missbräuchliche Verwendung der E-ID oder ist die Sicherheit der E-ID gefährdet, so kann fedpol ein Prüfverfahren durchführen. Es kann insbesondere die Identität der Inhaberin oder des Inhabers erneut prüfen lassen; die im Ausstellungsprozess erhobenen biometrischen Daten auswerten; die Inhaberin oder den Inhaber, betroffene Personen oder Dritte anhören.

fedpol kann eine E-ID von Amtes wegen widerrufen. Der Widerruf erfolgt automatisch und wird archiviert. Er wird im Basisregister vermerkt. Anhand der Widerrufsliste kann eine Verifikatorin feststellen, dass eine widerrufene E-ID nicht mehr gültig ist.

Art. 31 Betrieb des Informationssystems zur Ausstellung und zum Widerruf der E-ID

Absatz 1 und 2

Das fedpol führt täglich eine automatisierte Abfrage der in Artikel 26 Absatz 3 BGEID genannten Informationssysteme durch. Das EJPD regelt die Schnittstellen sowie die Funktionsweise des Informationssystems zur Ausstellung und zum Widerruf der E-ID.

4. Kapitel: Zugang der Anwendungen für Menschen mit Behinderungen

Art. 32

Das BIT ist verpflichtet, sicherzustellen, dass die Anwendung zum Vorweisen und Aufbewahren elektronischer Nachweise sowie die Anwendung zur Prüfung von elektronischen Nachweisen auch für Menschen mit Behinderungen zugänglich sind. Auch das fedpol hat die erforderlichen Massnahmen zu treffen, damit der Zugang der Anwendungen, die im Verfahren zum Bezug der E-ID oder zu deren Widerruf verwendeten werden, gewährleistet ist. Zu diesen Anwendungen zählen zum Beispiel die Benutzeroberflächen zur Dateneingabe, aber auch einzelne Prozessteile im Rahmen des Ausstellungsprozesses. Insbesondere müssen das BIT und fedpol bei wichtigen Aktualisierun-

gen der Systeme, die als «Releases» bezeichnet werden, den Zugang der Anwendungen berücksichtigen. Diese Massnahmen tragen dazu bei, digitale Inklusion zu fördern und den Zugang zu wichtigen Diensten für alle Personen zu gewährleisten.

5. Kapitel: Format elektronischer Nachweise sowie Standards und Protokolle für die Verfahren der Datenbekanntgabe

Art. 33 Veröffentlichung von Formaten und der Standards und Protokolle

Absatz 1

Ziel dieser Regelung ist es, eine zuverlässige und interoperable Grundlage für die sichere Verwendung von elektronischen Nachweisen und deren vertrauenswürdige Verifikation zu schaffen.

Elektronische Nachweise können in diesem Zusammenhang beispielsweise digitale Dokumente, Bescheinigungen oder andere Formen von Nachweisen sein, die in einem fälschungssicheren elektronischen Format übermittelt werden. Um diese Nachweise in unterschiedlichen Kontexten – sei es bei der behördlichen Kommunikation, der Übermittlung von Bescheinigungen oder der Verifikation – rechtssicher und eindeutig nachvollziehbar zu gestalten, ist es erforderlich, standardisierte technische Rahmenbedingungen festzulegen. Hierzu gehören insbesondere die Festlegung von Formaten, wie etwa Dokumentenformaten oder strukturierten Datenformaten, sowie von Standards und Protokollen, die die sichere Übertragung dieser Daten gewährleisten. Die Standards und Protokolle beinhalten vor allem die technischen und organisatorischen Empfehlungen zur Sicherstellung der Integrität und Authentizität von elektronischen Nachweisen sowie die Interoperabilität zwischen den am System angeschlossenen Akteuren und Akteurinnen.

Das BJ ist dabei verantwortlich für die Erstellung und Pflege des sicheren und interoperablen Rahmens, der die Nutzung elektronischer Nachweise in der Vertrauensinfrastruktur ermöglicht.

Absatz 2

Die Formate sowie die Standards und Protokolle sind vom BJ auf der Internetseite des Bundes zu veröffentlichen. Es kann dabei auch auf Webseiten verweisen, die es verwaltet, wie insbesondere auf GitHub. Die Veröffentlichung erfolgt in der Form von Empfehlungen (Best Practices). Die Best Practices beinhalten detaillierte Ausführungen, wie die elektronischen Nachweise sicher und effizient erstellt, geprüft und verwendet werden sollen. Die Veröffentlichung als Best Practices stellt sicher, dass alle Akteure und Akteurinnen denselben Standards folgen können, ohne zugleich individuelle Weiterentwicklungen oder Innovationen einzuschränken. Mit den Best Practices soll daher ein sicheres und interoperables System für die Verwendung und die Verifikation elektronischer Nachweise gefördert werden, das Vertrauen in die digitale Infrastruktur stärkt und eine breite und bedienungsfreundliche Nutzung ermöglicht.

Art. 34 Weiterentwicklung der Empfehlungen

Absatz 1 und 2

Mit der Veröffentlichung der Empfehlungen nach Artikel 33 (Best Practices) wird sichergestellt, dass die Formate und Standards kontinuierlich an die technischen Entwicklungen und rechtlichen Anforderungen durch das BJ angepasst werden können. Dies ermöglicht es auch privaten Akteurinnen und Akteuren, von den neuesten technologischen und rechtlichen Innovationen zu profitieren und ihre Systeme auf dem neuesten Stand zu halten.

Das BJ kann für die Weiterentwicklung der Best Practices interne und externe Sachverständige sowie dedizierte Fachgremien und Standardisierungsorganisationen beiziehen.

Absatz 3

Werden Änderungen an den Best Practices vorgenommen, sind diese ebenfalls zu veröffentlichen. Für die Veröffentlichung gilt dasselbe wie in Artikel 33 Absatz 2.

Art. 35 Verbindliche Formate, Standards und Protokolle

Absatz 1

Das EJPD kann in einer Departementsverordnung spezifische Formate für elektronische Nachweise sowie Standards und Protokolle für die Datenbekanntgabe als verbindlich erklären – dies für Systembeteiligte der Vertrauensinfrastruktur, insbesondere Ausstellerinnen und Verifikatorinnen elektronischer Nachweise, sowie für Anbieterinnen und Anbieter von Anwendungen nach Artikel 18 Absatz 4 und 5 BGEID. Dies kann beispielsweise erfolgen, wenn die bestehenden Formate und Standards nicht die erforderliche Interoperabilität zwischen verschiedenen Systemen und Akteurinnen und Akteuren gewährleisten. Fehlt diese Interoperabilität, können Daten nicht effizient und fehlerfrei zwischen den beteiligten Stellen ausgetauscht werden. Die verbindlichen Formate, Standards und Protokolle gelten in jedem Fall auch für die Anwendung des Bundes zur Aufbewahrung und Vorweisung von elektronischen Nachweisen nach Artikel 8 Absatz 1 BGEID.

Ein weiterer Grund für verbindliche Formate, Standards und Protokolle ist die Notwendigkeit, veraltete Versionen durch neue, sicherere und effizientere Versionen zu ersetzen. Zudem dient die verbindliche Festlegung dazu, einen allfälligen Standardisierungsprozess voranzutreiben und technische Fortschritte schneller in die Praxis umzusetzen. Ohne eine verbindliche Regelung könnte es zu Fragmentierungen und Ineffizienzen kommen, sofern zu viele unterschiedliche Lösungen verwendet werden.

Absatz 2

Bevor das EJPD ein Format, einen Standard oder ein Protokoll als verbindlich festlegt, wird es alle relevanten Akteurinnen und Akteure und Interessengruppen konsultieren.

Dies stellt sicher, dass die vorgeschlagenen Regelungen in der Praxis umsetzbar sind und von den betroffenen Parteien akzeptiert werden. Ziel dieser Konsultation ist es, die Praktikabilität der geplanten Änderungen zu überprüfen und mögliche Herausforderungen frühzeitig zu identifizieren.

Diese Konsultationen sind auch eine Möglichkeit, um den Standardisierungsprozess bzw. die Vereinheitlichung im Schweizer Ökosystem gemeinsam und konsolidiert zu fördern. Durch den Einbezug der interessierten und betroffenen Kreise wird eine breite Akzeptanz und eine möglichst reibungslose Umsetzung gewährleistet. Zudem wird eine konsolidierte und einheitliche Nutzung von Standards gefördert.

Absatz 3

Wenn das EJPD ein Format, einen Standard oder ein Protokoll verbindlich erklärt, tritt die Regelung frühestens drei Monate nach dieser Erklärung in Kraft. Diese Frist ermöglicht es den betroffenen Parteien, sich auf die neuen Vorgaben vorzubereiten. In dieser Zeit können sie ihre Systeme und Prozesse anpassen, um die Anforderungen zu erfüllen.

Je nach Umfang und Komplexität der Änderungen kann das EJPD jedoch auch eine längere Frist vorsehen, wenn die Verbindlichkeit einen grösseren Eingriff in bestehende Systeme oder Infrastruktur erfordert. Beispielsweise könnte eine Übergangsfrist von mehreren Monaten oder sogar Jahren notwendig sein, um eine umfassende Anpassung und Implementierung zu ermöglichen. Besonders wenn neue Technologien oder sicherere Formate eingeführt werden, ist es wichtig, den Akteurinnen und Akteuren genügend Zeit zu geben, um ihre bestehenden Systeme zu aktualisieren und die Kompatibilität kontinuierlich sicherzustellen. Diese flexiblen Übergangsfristen helfen dabei, den Umstellungsprozess ohne unnötige Störungen oder Verzögerungen durchzuführen.

In dringenden Fällen, wenn eine unmittelbare Gefährdung der Funktionsfähigkeit elektronischer Nachweise oder der Vertrauensinfrastruktur vorliegt, können vom BIT sofort die notwendigen Anpassungen vorgenommen werden. Grundlage hierfür bildet das Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (ISG)[11]. Solche Sofortmassnahmen sind insbesondere dann relevant, wenn Bedrohungen, Gefahren, Schwachstellen und Sicherheitslücken auftreten, die die Integrität oder Vertraulichkeit der Daten infrage stellen könnten. In solchen Fällen kann es erforderlich sein, schnell zu handeln, um grössere Schäden oder Sicherheitslücken zu vermeiden. In diesen Fällen ist es nicht erforderlich, bestimmte Formate, Standards oder Protokolle verbindlich zu erklären.

Art. 36 Vermerk betreffend Nichteinhaltung von Formaten, Standards und Protokollen im Vertrauensregister

[11] SR **128**

Abgesehen vom Verdacht auf unsachgemässe Verwendung der Vertrauensinfrastruktur oder elektronischer Nachweise kann ein Vermerk im Vertrauensregister auch dann erfolgen, wenn das BJ Kenntnis von der Nichteinhaltung von verbindlichen Formaten, Standards oder Protokollen erhält. In einem solchen Fall kann das BJ ein Prüfverfahren einleiten, um die technische und rechtliche Konformität zu überprüfen. Wird die Nichteinhaltung festgestellt, erfolgt der Vermerk für Ausstellerinnen und Verifikatorinnen im Vertrauensregister analog nach Artikel 18 und die Löschung nach Artikel 19. Dasselbe gilt für Dritt-Wallet-Anbieterinnen und Anbieter nach den Artikel 18 Absätzen 4 und 5 BGEID.

6. Kapitel: Gebühren

Art. 37 Gebühren betreffend die Register

Mit Inkrafttreten des BGEID wird es technisch und operationell möglich sein, den Einwohnerinnen und Einwohnern der Schweiz sowie den Auslandschweizerinnen und -schweizern ihre elektronische Identität (E-ID) und weitere digitale Nachweise (z. B. Strafregisterauszug, aber auch der elektronischen Führerausweis [mDL] oder im Gesundheitsbereich und im Kontext politischer Rechte) rasch und in einer hohen Qualität zur Verfügung zu stellen.

Die geschätzten Gesamtkosten für die Vertrauensinfrastruktur belaufen sich auf rund 20.8 Mio. Franken pro Jahr. Ungefähr 50% dieser Gesamtkosten machen die Betriebskosten für die Vertrauensinfrastruktur aus. Die Betriebskosten setzen sich dabei aus den Kosten für die Eintragung in das Basisregister, aus den Prüfungskosten der Anträge für die Eintragung und Aktualisierung von Daten in das Vertrauensregister sowie den übrigen Kosten für den Betrieb der Vertrauensinfrastruktur zusammen. Da in Bezug auf die Nutzung der Infrastruktur Annahmen getroffen werden müssen, wird die Höhe der Gebühren nach Inbetriebnahme regelmässig zu überprüfen sein.

Die jährlichen Kosten der Vertrauensinfrastruktur, die den Gebühren unterstellt sind, bestehen aus den anteiligen Personalausgaben des Fachbereichs E-ID im BJ sowie im BIT, den daraus berechneten direkten Personalkosten, den allgemeinen Personalkosten, den Arbeitsplatzkosten, dem internen Sach- und Betriebsaufwand beim BIT, der Lizenzkosten sowie den Abschreibungen.

Jährliche Kosten der Vertrauensinfrastruktur, die den Gebühren unterstellt werden:	
Direkte Personalkosten	CHF 3.96 Mio.
Allg. Personalkosten (Art. 4 Abs. 2 Bst. c AllgGebV (20%)	CHF 0.79 Mio.
Arbeitsplatzkosten (Art. 4 Abs 2 Bst. b (22 Arbeitsplätze); Betrag gem. Tabelle EFV Jahr 2025	CHF 0.31 Mio.
Sach- und Betriebsaufwand BIT	CHF 3.0 Mio.
Lizenzkosten	CHF 0.1 Mio.

Kalkulatorische Abschreibungen auf Anlagen (Vertrauensinfrastruktur)	CHF 2.67 Mio.
Total	**CHF 10.83 Mio.**

Von diesen Kosten zu unterscheiden sind die restlichen Kosten in Höhe von 9.93 Mio. Franken, die im Sinne des öffentlichen Interesses zum Betrieb der Vertrauensinfrastruktur nicht den Gebühren unterstellt werden. Der Bund hat ein Interesse daran, für Bevölkerung und Wirtschaft ein modernes Informatik- oder Kommunikationssystem zu entwickeln und zu betreiben.

Absatz 1

Das Verhältnis des Basisregisters zu den unter die Gebühren unterstellten Kosten der Vertrauensinfrastruktur wird auf ein Drittel geschätzt. Somit wird für das Basisregister mit einem Kostenaufwand von 3.61 Mio. Franken gerechnet. In erster Linie profitieren insbesondere die Behörden von der Vertrauensinfrastruktur sowie der Nutzung elektronischer Nachweise wie der E-ID. Weitere Nutzungen der Infrastruktur sind ebenfalls angedacht, insbesondere mit dem elektronischen Führerausweis (mDL), im Gesundheitsbereich und im Kontext politischer Rechte. Dies betrifft sowohl Bundesbehörden als auch kantonale Stellen. In erster Linie profitieren demnach die Behörden von der Vertrauensinfrastruktur sowie der Nutzung elektronischer Nachweise wie der E-ID. Gestützt auf diese Ausgangslage wird davon ausgegangen, dass etwa 60 % der Gesamtkosten für das Basisregister, also rund 2.17 Mio. Franken, durch den Betrieb im Zusammenhang mit der behördlichen Nutzung verursacht werden. Nach dem BGEID werden für Behörden allerdings keine Gebühren erhoben. Dennoch sind ihre Kostenanteile bei der Berechnung der Gebühr zu berücksichtigen. So entfallen auf die Nutzung durch die Privatwirtschaft die verbleibenden Kosten von 40 % (1.44 Mio. Franken). Für diese Nutzung wird eine Gebühr kalkuliert, die sich aus diesen restlichen Kosten von 1.44 Mio. Franken für das Basisregister und der erwarteten Anzahl an Eintragungen ableitet.

Bei der Festlegung der Gebühr werden nach Möglichkeit ein etwas längerer Planungshorizont abgedeckt und mögliche künftige Entwicklungen bereits einbezogen. Vor dem Hintergrund eines längeren Planungshorizonts wird prognostiziert, dass die jährlichen Eintragungen in das Basisregister im Schnitt 20% der gesamten Neueinträge in die kantonalen Handelsregister entsprechen werden[12]. Die Prognose von 20% vom Handelsregister als Anteil der jährlichen Neueintragungen im Basisregister basiert auf einer vorsichtigen Schätzung von Eintragungen, die sowohl die breitere Zielgruppe als auch die freiwillige Natur der Registrierung berücksichtigt. Es werden nur die Neueinträge berücksichtigt, da die Ausstellerinnen und Verifikatorinnen ihren jeweiligen Eintrag im Basisregister selbst verwalten, d. h. sie nehmen Änderungen und andere Anpassungen selbst vor. Die Nutzung des Basisregisters steht allerdings nicht nur Unternehmen zur

[12] Die durchschnittlichen Neueintragungen stützen sich auf die vom Eidgenössischen Amt für das Handelsregister zur Verfügung gestellten Vergleichstabellen der kantonalen Jahresberichte nach Artikel 5a HRegV (vgl. Handelsregister-Statistik).

Verfügung, die bereits im Handelsregister eingetragen sind, sondern auch anderen Unternehmen, die bislang nicht registriert sind, auch Einzelpersonen. Trotz dieser erweiterten Zielgruppe wird die tatsächliche Nutzung des Registers dennoch als eher moderat eingeschätzt. Die 20% reflektieren somit eine vorsichtige Einschätzung der tatsächlichen Beteiligung.

Somit ergibt sich aus den restlichen Gesamtkosten von 1.44 Mio. Franken und den prognostizierten Einträgen in das Basisregister eine Gebühr von 150 Franken.

Absatz 2

Gemäss Artikel 31 BGEID ist die Erhebung einer Gebühr vorgesehen, wenn die Ausstellerinnen und die Verifikatorinnen die Eintragung ihrer Daten in das Vertrauensregister beantragen. Anders als die Eintragung in das Basisregister erfordert die Bestätigung des Identifikators einer privaten Ausstellerin oder Verifikatorin im Vertrauensregister eine Prüfung des Antrags nach Artikel 10 oder eine Prüfung zur Aktualisierung der Daten im Vertrauensregister nach Artikel 11 Absatz 4. Die Gebühr für die Prüfung berechnet sich pauschal nach dem erwarteten Aufwand. Sie beträgt 350 Franken pro geprüften Antrag.

Art. 38 Gebühren für die Identitätsprüfung vor Ort

Absatz 1

Die Gebühren für die Identitätsprüfung vor Ort im Ausstellungsverfahren der E-ID wird innerhalb der folgenden Rahmenbedingungen durch die Kantone selbst festgelegt:

a. Wird nur eine E-ID beantragt, kann eine Gebühr von höchstens 29 Franken verlangt werden.

b. Wird die E-ID in Kombination mit einer Identitätskarte und / oder einem Pass beantragt, so kann eine zusätzliche Gebühr von höchstens 15 Franken erhoben werden, die neben den bereits festgelegten Gebühren für die Ausstellung der physischen Ausweisdokumente anfällt.

Diese Gebührenregelung sorgt für eine klare Strukturierung der Gebühren im Hinblick auf die verschiedenen Varianten der E-ID-Ausstellung und gleichzeitig dafür, dass die Kantone nicht mehr für die E-ID verlangen sollen, als Kosten für die Ausgestaltung der Identitätsprüfung vor Ort anfallen.

Absatz 2

Die konsularischen Vertretungen können für die Identitätsprüfung vor Ort nach Artikel 14 Absatz 3 der Verordnung vom 7. Oktober 2015[13] über die Gebühren des Eidgenössischen Departements für auswärtige Angelegenheiten eine Gebühr von höchstens 28 Franken erheben.

7. Kapitel: Schlussbestimmungen

Art. 39 Änderungen anderer Erlasse

Der Verordnungsentwurf schlägt die Änderung weiterer Rechtsakte vor. Diese Anpassungen zielen insbesondere darauf ab, die Nutzung der E-ID sowohl in der virtuellen als auch in der realen Welt zu fördern. Die E-ID muss immer als Identitätsnachweis akzeptiert werden, insbesondere durch die Behörden, unabhängig davon, ob die Identifizierung online oder vor Ort erfolgt. Die E-ID ersetzt nicht die physischen Identitätsdokumente, sollte jedoch als Alternative vorgelegt werden können. Durch die Anwendung zur Überprüfung elektronischer Nachweise können die Behörden beispielsweise eine E-ID bei direktem Kontakt mit einer Person einfach überprüfen. Sie müssen die E-ID akzeptieren, auch wenn dies im Rahmen eines Verfahrens geschieht, das keine Kopie eines Identitätsdokuments erfordert (Artikel 24 BGEID).

Art. 40 Inkrafttreten

Artikel 35 Absatz 2 Buchstabe b BGEID sieht die Möglichkeit einer späteren Bereitstellung des Systems für Sicherheitskopien (Artikel 15) vor. Dieses System soll der Inhaberin oder dem Inhaber ermöglichen, Sicherheitskopien ihrer oder seiner elektronischen Nachweise zu speichern. Es soll spätestens zwei Jahre nach Inkrafttreten dieser Verordnung eingerichtet werden. Auch die Erweiterung der Anwendung zur Überprüfung elektronischer Nachweise nach Artikel 16 (Check-App des Bundes) sowie die Identitätsprüfung vor Ort nach Artikel 24 müssen spätestens zwei Jahre nach Inkrafttreten der Verordnung umgesetzt werden.

4 Erläuterungen zu Anhang 1 (Änderung anderer Erlasse)

Mit dem BGEID und der Verordnung zum BGEID wird die Inhaberin oder der Inhaber einer E-ID sich entweder durch Vorweisung der E-ID oder – wie bisher – durch einen physischen Identitätsnachweis identifizieren können. Um insbesondere die Verwendung der E-ID zu ermöglichen, müssen verschiedene Verordnungen des Bundesrats geändert werden.

[13] SR **191.11**

Es ist zu beachten, dass auch einige Verordnungen des EJPD auf Ebene der zuständigen Ämter geändert werden müssen.

4.1 Verordnung vom 12. April 2006[14] über das Zentrale Migrationsinformationssystem

Art. 9 Bst. b Ziff. 9

Alle in der Schweiz lebenden ausländischen Staatsangehörigen werden im ZEMIS (Zentrales Migrationssystem) mit einheitlichen Personenangaben geführt. Sämtliche Funktionen und Tätigkeiten von der Einreise über den Aufenthalt bis zum Verlassen der Schweiz werden über ZEMIS abgewickelt. Mehr als 30'000 Mitarbeitende der Migrationsämter von Bund, Kantonen und einigen Gemeinden sowie verschiedener Arbeitsämter arbeiten mit dieser Anwendung.

Daten aus dem Ausländerbereich werden mithin neu auch durch ein Abrufverfahren dem Bereich «Staatliche Identitätsstelle» (SID) im Bundesamt für Polizei (fedpol) zugänglich gemacht, um die Aufgaben nach dem BGEID zu erfüllen.

Art. 10 Bst. b Ziff. 9

Daten aus dem Asylbereich werden durch ein Abrufverfahren ebenfalls dem Bereich «Staatliche Identitätsstelle» (SID) im Bundesamt für Polizei (fedpol) zugänglich gemacht, um die Aufgaben dem BGEID zu erfüllen.

Art. 18 Abs. 4 Bst. g

Das SEM vernichtet nicht archivwürdige Personendaten im ZEMIS (Zentrales Migrationsinformationssystem) gemäss folgender Regel: Biometrische Daten zum Ausländerausweis werden zwanzig Jahre nach der Erfassung gelöscht.

Anhang 1

Der tabellarisch dargestellte Datenkatalog wird um den Bereich «Staatliche Identitätsstelle» (SID) des Bundesamts für Polizei erweitert.

4.2 Verordnung vom 20 September 2002[15] über die Ausweise für Schweizer Staatsangehörige

Art. 28, Bst. l

[14] SR **142.513**

[15] SR **143.11**

Der Zweck der Datenbearbeitung in Artikel 28 soll in einem neuen Buchstaben l aufgenommen werden. Das Informationssystem Ausweisschriften ISA dient insbesondere der Identitätsprüfung bei der Ausstellung einer E-ID nach Artikel 16 BGEID.

Das ISA sammelt alle Daten zur Erstellung von Schweizerpässen und Identitätskarten und stellt diese den verantwortlichen Stellen für die Produktion der Dokumente zur Verfügung. Der Benutzerkreis in Bundesbehörden, kantonalen Passbüros und schweizerischen Auslandvertretungen umfasst mehrere hundert Personen.

Anhang 1 (Artikel 30 Absatz 1)

Die Berechtigungen der beteiligten Behörden zum Zugriff auf das ISA und der Umfang der Zugriffsrechte sind im Anhang 1 geregelt. Der Bereich Staatliche Identitätsstelle (fedpol SID) erhält dieselbe Berechtigung zur Bearbeitung oder Abfrage von im ISA gespeicherten Daten wie die zuständige Polizeistelle des Bundes (fedpol Pol; vgl. Artikel 12 Absatz 2 Buchstabe d und f sowie Absatz 3 AwG), ausser Unterschrift, Fingerabdrücke und Ausweiszustand. fedpol SID wird ausserdem folgende Daten erhalten: Einträge über Schriftensperre, Verlustanzeige/-revokation.

4.3 Verordnung vom 19. Oktober 2016[16] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes

Artikel 11 Absatz 5

Die private Postadresse durfte bisher nur in IAM-Systemen mit Privatpersonen und Vertreterinnen oder Vertretern von Organisationen nach Artikel 9 Buchstabe b IAMV bearbeitet werden. Neu darf die private Postadresse auch von Personen nach Artikel 8 IAMV (nicht aber Artikel 9 Buchstabe a IAMV) in den entsprechenden IAM-Systemen, Verzeichnisdiensten und dem zentralen Identitätsspeicher nach Artikel 13 IAMV bearbeitet werden, weshalb die Stellen mit ** gekennzeichnet werden. Als Einschränkung dürfen die mit ** gekennzeichneten Personendaten aber nur an Informationssysteme der zentralen Bundesverwaltung bekannt gegeben werden. Die Einhaltung dieser Einschränkung ist von den entsprechenden IAM-Systemen zu gewährleisten. Je nachdem ob ein nachgelagertes Informationssystem zur zentralen Bundesverwaltung gehört oder nicht, ist die private Postadresse in die Liste nach Artikel 15 Absatz 2 IAMV aufzunehmen. Eine Bekanntgabe der privaten Postadresse an einen externen Betreiber nach Artikel 17 IAMV ist beispielsweise nicht zulässig.

[16] SR **172.010.59**

Die Einschränkung betrifft nur die mit ** gekennzeichneten Stellen und gilt nur für die Daten von Personen nach Artikel 8. Sie gilt nicht für die private Postadresse von Personen nach Artikel 9 Buchstabe b IAMV, die schon bisher bearbeitet und in bestimmten Fällen beispielsweise auch externen Betreibern bekannt gegeben werden darf.

Artikel 19 Absatz 1

Die E-ID kann als elektronischer Identitätsnachweis, nicht aber als Zugangsberechtigung genutzt werden. Die E-ID ermöglicht es, die eigene Identität nachzuweisen.

Artikel 19 Absatz 3

Beim Vorweisen der E-ID wird der Inhalt der E-ID als Datenpaket nach Artikel 7 Absatz 1 BGEID an die Verifikatorin übermittelt.

Anhang Buchstabe g

Mit Einführung der E-ID müssen auch deren zusätzliche Informationen (E-ID Nummer, Aussteller und Ausstellungsdatum) von einem IAM-System bearbeitet werden dürfen. Diese müssen für Rechercheszenarien auch in den entsprechenden Audit-Speichern gespeichert werden können.

Die Bearbeitung anderer Attribute der E-ID werden bereits von anderen Buchstaben des Anhangs autorisiert.

4.4 Verordnung vom 19 Oktober 2022[17] über das Strafregister-Informationssystem VOSTRA

Art. 52 Absatz 2

In Artikel 52 Absatz 2 und 3 StReV werden die Anforderungen an den Identitätsnachweis nach Artikel 54 Absatz 3 StReG definiert. Anerkannt werden nach Artikel 52 Absatz 2 StReV grundsätzlich nur die offiziellen Ausweisdokumente Pass, Identitätskarte und Ausländerausweis. Im Online-Bestellverfahren wird auch die elektronische Identität (E-ID) nach dem E-ID Gesetz vom 20. Dezember 2024 akzeptiert.

[17] SR **331**

4.5 Verordnung vom 27. Oktober 1976[18] über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr

Art. 11 Abs. 3 und 4

Nutzung der E-ID bei Ausweisgesuchen
Die Liste der Identitätsnachweise in Artikel 11 Absatz 3 VZV soll um die E-ID ergänzt werden. Die Nutzung der E-ID ermöglicht die weitere Digitalisierung der Gesuchseinreichung um Lernfahrausweise, Führerausweise oder Bewilligungen zum berufsmässigen Personentransport, sofern die Kantone davon Gebrauch machen und entsprechende Möglichkeiten einrichten möchten. Weil die Identität bei Erteilung einer E-ID gemäss BGEID bereits überprüft wird (online durch das fedpol [Artikel 17 Absatz 1 Buchstabe a BGEID] oder persönlich bei einer dafür bezeichneten Stelle oder Behörde [Artikel 17 Absatz 1 Buchstabe b BGEID]), erübrigt sich eine persönliche Vorsprache in diesem Fall. Damit die Behörden auch elektronisch eingehende Gesuche bearbeiten können, soll die mit der Entgegennahme betraute Person die Identität in einer dafür geeigneten elektronischen Form bestätigen können. Daher wird eine Ergänzung in Artikel 11 Absatz 4 VZV sowie in Anhang 4 VZV vorgeschlagen.

4.6 Verordnung vom 30 November 2018[19] über das Informationssystem Verkehrszulassung

Anhang 1 und Anhang 2

E-Mail-Adresse und Telefonnummern
Das Führen der E-Mail-Adresse sowie der Telefonnummern (worunter Mobil- wie auch Festnetznummern fallen können) stellt im digitalen Kontakt zwischen Behörden und Bürgerinnen und Bürgern einen wesentlichen Bestandteil der Kommunikation dar und trägt zur beidseitigen administrativen Erleichterung bei. Sie sind notwendig für den Ausstellungsprozess des elektronischen Lernfahrausweis (eLFA) und werden inskünftig auch für weitere elektronische Nachweise und Dokumente benötigt.

Gemäss Artikel 14 der Verkehrszulassungsverordnung (VZV)[20] übermitteln die Zulassungsbehörden dem Subsystem IVZ-Personen die Personalien der Gesuchstellenden. Entsprechend ist das «Gesuch um die Erteilung eines Lernfahr- oder Führerausweises oder der Bewilligung zum berufsmässigen Personentransport» gemäss Anhang 4 der VZV mit der E-Mail-Adresse und der Mobil-Telefonnummer zu ergänzen.

Damit die Attribute im Informationssystem Verkehrszulassung (IVZ) geführt werden dürfen, ist der Sammelbegriff «Telefonnummern» und die «E-Mail-Adresse» in der

[18] SR **741.51**
[19] SR **741.58**
[20] SR **741.51**

Verordnung über das Informationssystem Verkehrszulassung (IVZV)[21] wie folgt aufzunehmen: Im Anhang 1 unter Ziffer 22 und im Anhang 2 unter Ziffern 112, 212, 222, 223 und 232.

AHV-Nummer
Die AHV-Nummer ist eindeutiger Identifikator einer in der Schweiz wohnenden (oder sozialversicherungstechnisch oder erwerbsmässig gemeldeten) Person. Sie erweist sich daher als nützlich zur Optimierung von administrativen Abläufen. Viele kantonale Behörden nutzen seit der Revision des AHV-Gesetzes die AHV-Nummer bereits als eindeutigen Identifikator. Dies dient dem datenschutzrechtlichen Prinzip der Datenrichtigkeit und senkt den Verwaltungsaufwand, wodurch die Vollzugsbehörden entlastet werden. Kostenintensive Arbeiten zur Behebung von Namens-Verwechslungen und unangenehme Konsequenzen für Betroffene können damit weitestgehend vermieden werden.

Entsprechend ist die IVZV mit der AHV-Nummer im Anhang 1 unter Ziffer 21 und im Anhang 2 unter Ziffer 111 und 211 zu ergänzen.

Geschäftliche Identifikationsnummern (UID, BUR-Nummer, Geschäftspartner-Nummer)
Unter dem Sammelbegriff «geschäftliche Identifikationsnummern» werden eindeutige Identifikatoren für juristische Personen zusammengefasst, welche im Zuge der Änderungen zur E-ID rein vollständigkeitshalber ergänzt werden sollen.

- Die Unternehmens-Identifikationsnummer (UID) und die Nummer aus dem Betriebs- und Unternehmensregister (BUR-Nummer), gelten als Pendant zur AHV-Nummer bei juristischen Personen und dienen somit als eindeutiger Identifikator. Das Bundesamt für Zoll und Grenzsicherheit (BAZG) plant im Rahmen der Rechnungsstellung zur leistungsabhängigen Schwerverkehrsabgabe (LSVA)[22] die UID und BUR-Nummern zu nutzen und diese für einen effizienten Vollzug aus dem IVZ beziehen zu können.[23] Mit der Verwendung der UID und BUR-Nummer kann zudem, wie bei der AHV-Nummer, die Datenqualität weiter optimiert werden.

- Die Geschäftspartnernummer ist der Schlüssel, welcher die Geschäftspartner bei der Fakturierung eindeutig identifiziert und die Stammdatenpflege vereinfacht.

[21] SR **741.58**

[22] SR **641.81**

[23] Im Rahmen von Artikel 89d Buchstabe f Strassenverkehrsgesetz (SVG, SR **741.01**)

Der Sammelbegriff «geschäftliche Identifikationsnummern» ist deshalb wie folgt in der IVZV aufzunehmen: Im Anhang 1 unter Ziffer 21 und im Anhang 2 unter Ziffern 212, 221, 222, 231, 232 und 241.

Korrespondenzsprache
Der Begriff «Sprache» ist unklar und soll durch «Korrespondenzsprache» präzisiert werden in der IVZV im Anhang 1 unter Ziffer 22.

4.7 Verordnung vom 15. November 2017[24] über die Überwachung des Post- und Fernmeldeverkehrs

Artikel 20a Absatz 1, Einleitungssatz und Buchstaben b-d, Absatz 2 Buchstabe a, Einleitungssatz und Ziffer 3, Absätze 4 und 5

Die Identitätsprüfung einer natürlichen Person ist für Mobilfunkdienste unerlässlich. Die Verfahren zur Identitätsprüfung sind nicht geregelt. Eine Identifizierung in Anwesenheit der natürlichen Person, per Video oder online ist möglich, wobei im letzteren Fall die im FINMA-Rundschreiben 2016/7 «Identifikation per Video und Online» festgelegten Sicherheits- und Qualitätsnormen eingehalten werden müssen. Um eine sichere Identifikation zu gewährleisten, muss der Identitätsnachweis zum Zeitpunkt seiner Erfassung gültig sein, d. h. am Tag, an dem der entsprechende Nachweis dem Anbieter oder Verkäufer vorgelegt wird bzw. online genutzt wird.[25]

Artikel 20*a* VÜPF wird geändert, um den elektronischen Identitätsnachweis (E-ID) zu berücksichtigen, der von fedpol für natürliche Personen ausgestellt wird und mit der neuen BGEID eingeführt wird. In Absatz 1 wird daher die Aufzählung der Dokumente um die E-ID (Buchstabe d) ergänzt.

Die E-ID besteht aus einem Datensatz, der als elektronischer Identitätsnachweis dient (Artikel 13 BGEID). Daher wird der allgemeinere Begriff «Identitätsnachweis» bevorzugt, der den Begriff «Dokument» im einleitenden Satz ersetzt. In Absatz 2 besteht die einzige Änderung darin, dass «Identitätsnachweis» anstelle von «Dokument» verwendet wird, was sich vor dem Hintergrund der E-ID besser eignet. Absatz 3 bleibt unverändert.

Absatz 4 Satz 1 bleibt unverändert. Der Begriff «Dokument» kann weiterhin verwendet werden, da er sich auf die in Absatz 1 Buchstabe a bis c genannten Dokumente bezieht und nicht auf die E-ID. Ein zweiter Satz wird hinzugefügt, um den spezifischen Informationsbedarf im Falle der Verwendung einer E-ID zu berücksichtigen. Es werden nur die Daten nach Absatz 2 sowie das Foto erhoben, anstelle einer Kopie

[24] SR **780.11**

[25] Siehe den erläuternden Bericht vom 15.11.2023 zu den Teilrevisionen von Ausführungserlassen des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), Art. 20*a*, S. 20 ff.

des physischen Identitätsdokuments. Tatsächlich enthält die E-ID Informationen, die der Pass, der Personalausweis oder die Aufenthaltsgenehmigung nicht enthalten, insbesondere die AHV-Nummer (Artikel 15 Absatz 1 Buchstabe i, BGEID). Es wäre unverhältnismässig und im Widerspruch zu Artikel 6 DSG, von der Person, die sich mit einer E-ID identifiziert, diese Information zu verlangen, wenn sie dies mit einem physischen Identitätsdokument nicht hätte tun müssen.

Darüber hinaus müssen die für die Prüfung der Authentizität und Integrität erforderlichen Daten wie die elektronische Unterschrift (Artikel 5 Absatz 2 BGEID) ebenfalls erfasst werden. Tatsächlich ist ein Anbieter oder Verkäufer nicht verpflichtet, ein Identitätsdokument gründlich zu prüfen, um dessen Authentizität zu bestätigen, sondern muss das vorgelegte Dokument nur dann akzeptieren, wenn dessen Authentizität plausibel erscheint.[26] Ein nur oberflächlicher Kontrollmechanismus ist erforderlich. Bei der E-ID würde das Fehlen jeglicher Kontrolle es jedoch ermöglichen, fehlerhafte Daten zu registrieren oder ein Foto einer anderen Person bei einem Anbieter oder Verkäufer, der nicht genau hinsehen würde, vorzulegen. Darüber hinaus wird die Produktion dieser Verifizierungsdaten voraussichtlich schnell erfolgen, sodass ihre Erhebung und Übermittlung nicht mehr Zeit in Anspruch nehmen sollte als bei einem physischen Dokument.

Absatz 5 enthält die Regelung des zweiten Satzes des früheren Absatzes 4 mit den Anpassungen durch die E-ID. Um die Lesbarkeit zu verbessern, wurde ein neuer Absatz 5 eingeführt. Hinsichtlich der erhobenen Daten wurde der Verweis auf die betroffenen Absätze daher um Absatz 4 ergänzt. Die Frist für die Übermittlung der Daten vom Verkäufer an die Anbieterinnen von Fernmeldediensten bleibt unverändert (drei Tage).

4.8 Postverordnung vom 29. August 2012[27]

Art. 35e Abs. 2 Bst. c und Abs. 3

Die Nutzerinnen und Nutzer des hybriden Zustellsystems, namentlich Absenderinnen und Absender sowie Empfängerinnen und Empfänger, müssen sich gegenüber der Post identifizieren und authentifizieren (Absatz 1). Für die Identifikation der Personen kann nach Buchstabe c die E-ID verwendet werden. Damit wird präzisiert, dass als elektronischer Identitätsnachweis im Rahmen der Grundversorgung die E-ID zur Anwendung kommt. Mit der E-ID erübrigt sich sodann, dass die Eidgenössische Postkommission bestimmen muss, welche elektronischen Identitätsnachweise zur Identifikation der Nutzerinnen und Nutzer eingesetzt werden können (Absatz 3).

[26] Siehe den oben genannten erläuternden Bericht, Art. 20*a*, S. 20 ff.

[27] SR **783.01**

4.9 Verordnung vom 9. März 2007[28] über Fernmeldedienste

Art. 41 Abs. 5 Bst. b

Mit dem E-ID-Gesetz wird die Basis für die Herausgabe von elektronischen Identifizierungsmitteln geschaffen, die es dem Einzelnen ermöglichen, sich aufgrund staatlich bestätigter Daten im digitalen Raum zu identifizieren. Es wird somit die Grundlage für eine E-ID geschaffen, womit die Einzelnen den Nachweis ihrer Identität erbringen können. Bei der Altersprüfung in Zusammenhang mit der obligatorischen Sperre der Mehrwertdienste für Minderjährige kann der Identitätsnachweis neu auch mit einer E-ID erbracht werden.

4.10 Verordnung vom 6. Oktober 1997[29] über die Adressierungselemente im Fernmeldebereich

Art. 4 Abs. 1ter und Art. 4 Abs. 1ter Bst. a

Mit dem E-ID-Gesetz wird die Basis für die Herausgabe von elektronischen Identifizierungsmitteln geschaffen, die es dem Einzelnen ermöglichen, sich aufgrund staatlich bestätigter Daten im digitalen Raum zu identifizieren. Es wird somit die Grundlage für eine E-ID geschaffen, womit die Einzelnen den Nachweis ihrer Identität erbringen können. Bei der Zuteilung von Adressierungselementen kann der Nachweis zur Überprüfung der Identität einer Gesuchstellerin oder eines Gesuchstellers neu auch mit einer E-ID erbracht werden.

4.11 Verordnung vom 5. November 2014[30] über Internet-Domains

Art. 24 Abs. 3 Bst. a

Mit dem E-ID-Gesetz wird die Basis für die Herausgabe von elektronischen Identifizierungsmitteln geschaffen, die es dem Einzelnen ermöglichen, sich aufgrund staatlich bestätigter Daten im digitalen Raum zu identifizieren. Es wird somit die Grundlage für eine E-ID geschaffen, womit die Einzelnen den Nachweis ihrer Identität erbringen können. Bei der Zuteilung von Domain-Namen kann der Nachweis zur Überprüfung

[28] SR **784.101.1**

[29] SR **784.104**

[30] SR **784.104.2**

der Identität einer gesuchstellenden Person sowie der Zuteilungsvoraussetzungen neu auch mit einer E-ID erbracht werden.

4.12 Fortpflanzungsmedizinverordnung vom 4. Dezember 2000[31]

Art. 21 Abs. 2

Der Identitätsnachweis des Gesuchstellers oder der Gesuchstellerin kann grundsätzlich durch die Einreichung einer Kopie eines Identitätsdokuments (Reisepass, Identitätskarte, gleichwertiger Ausweis) oder durch die Verwendung einer E-ID nach dem BGEID erfolgen. Diese Möglichkeit, eine Kopie des Identitätsdokuments online einzureichen, hat sich bereits bei der Bestellung von Strafregisterauszügen bewährt. Mit der Einführung der E-ID wird zusätzlich eine digitale Variante des Identitätsnachweises ermöglicht, die keine Einreichung einer Kopie erfordert.

4.13 Verordnung vom 22. März 2017[32] über das elektronische Patientendossier

Der Herausgeber eines Identifikationsmittels, das für den Zugriff auf das elektronische Patientendossier (EPD) notwendig ist, muss die Identität der antragstellenden Person überprüfen. Dieser Identitätsnachweis soll künftig auch mit der E-ID erbracht werden können.

Mit dem Erlass des BGEID wird das Bundesgesetz vom 19. Juni 2015[33] über das elektronische Patientendossier (EPDG) dahingehend geändert, dass nur noch private Herausgeber von Identifikationsmitteln durch eine anerkannte Stelle zertifiziert werden müssen (Artikel 11 Buchstabe c EPDG). Kantone als Herausgeber von Identifikationsmitteln[34] werden demgegenüber nicht zertifiziert. Dennoch müssen von Kantonen herausgegebene Identifikationsmittel dieselben Anforderungen erfüllen wie Identifikationsmittel, die von Privaten herausgegeben werden. Verantwortlich für die Einhaltung dieser Anforderungen sind die Kantone.

Die von Kantonen herausgegebenen Identifikationsmittel sollen wie die von privaten Herausgebern herausgegebenen Identifikationsmittel dazu benutzt werden, dass sich Gesundheitsfachpersonen sowie Patientinnen und Patienten gegenüber dem System des EPD authentifizieren können. Auch das von der Bundeskanzlei betriebene System,

[31] SR **810.112.2**

[32] SR **816.11**

[33] SR **816.1**

[34] Die Kantone Genf und Waadt stellen bereits heute Identifikationsmittel für den Zugriff auf das EPD zur Verfügung.

das auf der Grundlage der E-ID die Authentifizierung natürlicher Personen ermöglicht (AGOV), soll künftig dafür eingesetzt werden können.

Art. 9 Abs. 2 Bst. e

Die Mittel, mit denen sich Gesundheitsfachpersonen für den Zugriff auf das EPD authentifizieren können, werden um Identifikationsmittel, die von Kantonen herausgegeben werden, erweitert. Ebenfalls zugelassen ist die Authentifizierung via AGOV.

Art. 16

Die Mittel, mit denen Patientinnen und Patienten ihre Einwilligung für die Erstellung eines EPD bestätigen können, werden um Identifikationsmittel, die von Kantonen herausgegeben werden, erweitert (*Buchstabe b*). Ebenfalls zugelassen ist die Bestätigung der Einwilligung via AGOV (*Buchstabe c*).

Art. 17 Abs. 1 Bst. c

Die Mittel, mit denen sich Patientinnen und Patienten für den Zugriff auf das EPD authentifizieren können, werden um Identifikationsmittel, die von Kantonen herausgegeben werden, erweitert. Ebenfalls zugelassen ist die Authentifizierung via AGOV.

Art. 24 Abs. 1

Die Person, die ein Identifikationsmittel für den Zugriff auf das EPD beantragt, kann sich gegenüber dem Herausgeber von Identifikationsmitteln neu auch mittels E-ID ausweisen.

Art. 27a Von Kantonen herausgegebene Identifikationsmittel

Da nur noch private Herausgeber von Identifikationsmitteln zertifiziert werden müssen (Artikel 11 Buchstabe c EPDG), muss geregelt werden, wer die Verantwortung dafür trägt, dass nur sichere Identifikationsmittel für die Authentifizierung beim Zugriff auf das EPD verwendet werden. *Absatz 1* weist diese Verantwortung den Kantonen, als deren Herausgeber, zu. Die Kantone müssen sicherstellen, dass die von ihnen herausgegebenen Identifikationsmittel den Anforderungen gemäss Artikel 23–27 EPDV sowie den Konkretisierungen nach Artikel 31 Absatz 2 und 3 genügen. Die Konkretisierungen befinden sich im Anhang 8 der Verordnung des EDI vom 22. März 2017[35] über das elektronische Patientendossier (EPDV-EDI).

Die Kantone melden die von ihnen herausgegebenen Identifikationsmittel dem Bundesamt für Gesundheit (BAG) (*Absatz 2*). Dieses sorgt laut *Absatz 3* dafür, dass diese

[35] SR **816.111**

Identifikationsmittel – analog der Veröffentlichung der Zertifikate der privaten Herausgeber von Identifikationsmitteln nach Artikel 33 Absatz 2 – publiziert werden.

Die Schutzklausel bezüglich von zertifizierten Herausgebern herausgegebenen Identifikationsmitteln (Artikel 37 Absatz 1 Buchstabe b) gilt auch für Identifikationsmittel, die von Kantonen herausgegeben werden (Absatz 4). Das BAG kann von den Kantonen die Unterlagen, die für die Beurteilung der Umstände nötig sind, einfordern.

Art. 28 Abs. 2

Es müssen nur die privaten Herausgeber von Identifikationsmitteln zertifiziert werden. Die Akkreditierung gilt dementsprechend auch nur für Stellen, die diese privaten Herausgeber von Identifikationsmitteln zertifizieren. *Absatz 2* wird dahingehend präzisiert.

Art. 31 Sachüberschrift und Abs. 1

Nur private Herausgeber von Identifikationsmitteln müssen zertifiziert werden. Für von Kantonen herausgegebene Identifikationsmittel sind diese verantwortlich. Die *Sachüberschrift* und *Absatz 1* werden dahingehend präzisiert.

Art. 32 Abs. 3

Die Zertifizierungsstelle erteilt das Zertifikat nur privaten Herausgebern von Identifikationsmitteln, sofern die jeweiligen Anforderungen erfüllt sind. Kantonale Herausgeber von Identifikationsmitteln werden nicht zertifiziert, erhalten also auch kein Zertifikat. *Absatz 3* wird dahingehend präzisiert.

Art. 36 Abs. 1

Nur private Herausgeber von Identifikationsmitteln müssen der Zertifizierungsstelle wesentliche technische oder organisatorische Anpassungen melden. Diese Pflicht gilt nicht für kantonale Herausgeber von Identifikationsmittel, denn für die kantonalen Identifikationsmittel trägt der Kanton die Verantwortung. *Absatz 1* wird dahingehend präzisiert.

4.14 Verordnung vom 23. November 2016[36] über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

Artikel 5 Absatz 1bis

[36] SR **943.032**

Anbieterinnen von Zertifizierungsdiensten müssen die genaue Identität der Personen feststellen, die einen Antrag auf Ausstellung eines geregelten Zertifikats stellen (Artikel 9 Absatz 1 des Bundesgesetzes über die elektronische Signatur [ZertES, SR 943.03]). Die antragstellende Person hat in der Regel persönlich bei einer anerkannten Zertifizierungsdienstanbieterin vorzusprechen (Artikel 5 Absatz 1 VZertES). Die Pflicht zur persönlichen Vorsprache entfällt, wenn die Identität mit einer E-ID nachgewiesen wird. Mit diesem neuen Absatz ist der Sachverhalt bezüglich der Identifikation mit der E-ID nochmals geklärt.

Artikel 6 Absatz 1

Die Pflicht einer Person, die ein geregeltes Zertifikat für eine UID-Einheit beantragt, die keine natürliche Person ist, zur Vorlage eines Reisepasses, einer schweizerischen Identitätskarte oder eines für die Einreise in die Schweiz anerkannten Identitätsausweises wird dahingehend geklärt, dass auch eine nach dem E-ID-Gesetz ausgestellte E-ID verwendet werden kann.

4.15 Verordnung vom 11. November 2015[37] über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung

Art. 17 Abs. 3 Bst. b und 3bis

Artikel 17 Absatz 3 GwV legt für die Händlerinnen und Händler nach Artikel 2 Absatz 1 Buchstabe b GwV dar, nach welchem Verfahren sie die Identifizierung der Vertragspartei nach den geldwäschereirechtlichen Vorschriften vorzunehmen haben.

In der Praxis werden nur gültige Ausweise zur Identifizierung der Vertragspartei akzeptiert. Dies wird durch die interne und externe Revision geprüft. Buchstabe b soll daher am Ende um «… und gültig ist» ergänzt werden, damit die geltende Praxis abgebildet ist und der Verordnungstext mit dem neuen Absatz 3bis Buchstabe b übereinstimmt.

Im Sinne der Klarheit soll mit dem neuen Absatz 3bis in Artikel 17 GwV präzisierend ergänzt werden, dass die Identifizierung der Vertragspartei ebenfalls über die nach dem Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise erstellte E-ID erfolgen kann.

Davon unabhängig ergeben sich für den Einsatz der E-ID zur Identifizierung von Vertragsparteien durch Finanzintermediäre (Artikel 2 Absatz 1 Buchstabe a GwV) die Anwendungsmöglichkeiten aus den Vorgaben der Eidg. Finanzmarktaufsicht FINMA. Der Einsatz der E-ID zur Identifizierung der Vertragsparteien von Handelsprüfern und

[37] SR **955.01**

ihren Gruppengesellschaften, die gewerbsmässig mit Bankedelmetallen handeln (Artikel 42bis EMKG) und ebenfalls als Finanzintermediäre gelten (Artikel 2 Absatz 2 Buchstabe g GwG), ergibt sich aus der GwV-BAZG (vgl. Artikel 17 Absatz 1 Buchstabe d GwG und Artikel 42ter Absatz 4 EMKG).

Ebenfalls unabhängig von Artikel 17 Absatz 3bis GwV ist die Möglichkeit, die E-ID anzuwenden zur Prüfung der Identität von Kunden, von denen der Inhaber oder die Inhaberin einer Schmelzbewilligung oder Ankaufsbewilligung Schmelzgut entgegennimmt (Artikel 168*a* Absatz 2 bzw. 172*e* Absatz 1 EKMV sowie die noch zu erlassenden Richtlinien und Weisungen).

5 Auswirkungen

5.1 Auswirkungen auf den Bund

Mit dem vorliegenden Verordnungsentwurf werden keine zusätzlichen finanziellen oder personellen Auswirkungen erwartet, die über den bereits im Rahmen des Programms E-ID festgelegten Ressourcenbedarf für den Aufbau, den Betrieb und die Weiterentwicklung von Vertrauensinfrastruktur, E-ID-Ausstellung und die E-ID-Pilotprojekte von 2023–2028 hinausgehen.

5.2 Auswirkungen auf Kantone und Gemeinden

Neben der Beantragung und Ausstellung der E-ID über einen Online-Kanal ist die Identitätsprüfung für die E-ID auch vor Ort in einem kantonalen Erfassungszentrum möglich. Damit ist es für Interessierte möglich, ausschliesslich zur Identitätsprüfung der E-ID einen Vor-Ort-Termin wahrzunehmen, zum Beispiel um die Speicherung von zusätzlichen biometrischen Daten zu umgehen (Variante Solo), oder auch den Besuch bei der Behörde in Kombination mit dem Antrag zur Ausstellung physischer Dokumente zu machen (Variante Ausweis+).

Basierend auf internationalen Erfahrungen und anhand grober Schätzungen geht man für die Variante Solo von maximal 1 Prozent aller potenziellen E-ID-Nutzerinnen und Nutzer aus. Bei der Variante Ausweis+ schätzt man, dass insbesondere auf Grund der zusätzlichen Gebühren nur 5 Prozent der Personen, die für eine Ausweiserneuerung bei der Behörde vorbeikommen, sich zusätzlich für den direkten Bezug der E-ID entscheiden; das sind rund 40’000 Fälle pro Jahr bei den Passbüros. Die Variante Ausweis+ wird aufgrund der Antrags-Prozesse nur für Antragstellende von Schweizer Identitätskarte und Schweizer Pass möglich sein.

5.3 Auswirkungen auf die Volkswirtschaft

Die digitale Transformation der Schweiz schreitet voran. Immer mehr Geschäfte können online abgewickelt werden. Es ist immer weniger nötig, persönlich vorzusprechen. Es wird vermehrt erwartet, dass verschiedene Geschäfte elektronisch, vorzugsweise auf einem Smartphone, erledigt werden können. Mit dem BGEID und den vorliegenden Ausführungsbestimmungen wird die Grundlage für die Verwendung von elektronischen Nachweisen im virtuellen Geschäftsverkehr gelegt. Sie schafft die Voraussetzungen für ein Ökosystem, das es ermöglicht, auf gesicherte Weise verschiedene elektronische Nachweise auszustellen, einzusetzen und vorzuweisen. Es handelt sich um eine Reihe von Normen und Standards, Prozessen, Konzepten und Infrastrukturkomponenten, die das Vertrauen in die digitalen Prozesse herstellen, deren Konformität gewährleisten und die von einem breiten Publikum akzeptiert und verwendet werden. Mit der E-ID können Behörden und Unternehmen für eine Vielzahl von Online-Diensten dieselben Formate verwenden. Für die Nutzer und Nutzerinnen solcher Dienste verringert sich die Anzahl der verschiedenen Anmeldungen. Ausserdem trägt dies zur Datensparsamkeit sowie zum Schutz der Privatsphäre bei. Durch die Festlegung von Standards und die Minimierung der Hürden für die Nutzung von Online-Diensten ergeben sich mithin bedeutende Chancen für die Wirtschaft und für öffentliche Dienstleistungen zur Innovation.

5.4 Auswirkungen auf die Gesellschaft

Anerkannte elektronische Identitätsnachweise tragen in einer vernetzten Gesellschaft zum Schutz der Identität der Inhaberinnen und Inhaber bei. Ein Missbrauch der Identität einer Person, der potenziell problematische Folgen haben kann, wird deutlich erschwert. In den Anwendungen des Bundes für die Aufbewahrung, Vorweisung und Überprüfung von elektronischen Nachweisen wird den Nutzerinnen und Nutzern die Möglichkeit zur Verfügung stehen, die Identität von Ausstellerinnen und Verifikatorinnen von elektronischen Nachweisen zu überprüfen. Die Anwendungen sollten so benutzerfreundlich wie möglich sein, damit die Verwendung elektronischer Nachweise für alle in der Bevölkerung zugänglich und einfach ist.

Damit die Förderung der digitalen Resilienz und der digitalen Souveränität sichergestellt ist, wird der Ansatz der selbstbestimmten Identität verfolgt. Dies erlaubt eine dezentrale Datenhaltung bei der einzelnen Nutzerin und dem einzelnen Nutzer. Der Austausch von Daten erfolgt ohne Umwege über eine zentrale Instanz direkt zwischen den an einer Transaktion beteiligten Parteien.

6 Rechtliche Aspekte

6.1 Informationssicherheit

Der Missbrauch von Informationen und die Störung der Vertrauensinfrastruktur und des Informationssystems zur Ausstellung und zum Widerruf der E-ID können wesentliche Interessen der Schweiz und die Rechte von Personen schwerwiegend beeinträchtigen sowie die gesetzliche Aufgabe zur Sicherstellung der Funktionsfähigkeit der Vertrauensinfrastruktur und des Informationssystems gefährden. Grundlage für die bestmögliche Sicherstellung der Informationssicherheit bilden dabei das Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (ISG)[38] und die zugehörige Verordnung (ISV)[39].

Das BJ und das BIT sind bezüglich der Vertrauensinfrastruktur und fedpol im Zusammenhang mit dem Informationssystem zu Ausstellung und zum Widerruf der E-ID dazu verpflichtet, dafür zu sorgen, dass Verletzungen der Informationssicherheit rasch erkannt, deren Ursachen abgeklärt und allfällige Auswirkungen minimiert werden. Hierzu treffen die verpflichteten Behörden die erforderlichen Massnahmen, um Sicherheitsvorfälle oder Sicherheitslücken zu identifizieren (wie z. B. durch regelmässige Auswertung von Log Files). Liegt ein Sicherheitsvorfall oder eine -lücke vor, nimmt das BIT im Kontext der Vertrauensinfrastruktur und fedpol bezüglich des Informationssystems die erforderlichen Sofortmassnahmen vor, um die allfälligen Auswirkungen auf die Informationssicherheit zu minimieren. Sicherheitsvorfälle oder Sicherheitslücken liegen im Kontext der Vertrauensinfrastruktur und der E-ID insbesondere vor, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit der elektronischen Nachweise oder der Vertrauensinfrastruktur bzw. des Informationssystems gefährdet oder beeinträchtigt sind; schwerwiegende Betriebsstörungen drohen oder eingetreten sind; oder Schwächen oder Fehler im System bestehen, die eine erhebliche Cyberbedrohung darstellen.

Im vorliegenden Verordnungsentwurf ist eine besonders detaillierte Regelung zum Umgang mit Gefährdungen der Informationssicherheit nicht erforderlich. Der Grund dafür ist, dass bereits das ISG und die ISV die rechtlichen Grundlagen bieten, die für die Behandlung solcher Gefährdungen notwendig sind. In ähnlicher Weise wie beim DSG wird auch hier auf die bestehende Systematik des Rechts hingewiesen. Das bedeutet, dass die bestehenden Regelungen in den relevanten Gesetzen bereits ausreichen, um den sicheren Umgang mit Risiken in der Informationssicherheit zu gewährleisten.

[38] SR **128**

[39] SR **128.1**

6.2 Datenschutz

Die Regeln des Datenschutzrechts (DSG und zugehörige Verordnungen) gelten für alle. Natürliche Personen, Ausstellerinnen und Verifikatorinnen des privaten Sektors unterliegen den Bestimmungen für Private. Der Bund (fedpol und andere Behörden) sowie die Ausstellerinnen und Verifikatorinnen des öffentlichen Sektors unterliegen den Bestimmungen für Bundesorgane. Im vorliegenden Verordnungsentwurf wird nicht auf die einschlägigen Bestimmungen des DSG verwiesen, um Wiederholungen zu vermeiden und die Auslegung nicht zu erschweren. Das BGEID präzisiert bereits, wie der Datenschutz im Kontext der E-ID umgesetzt wird. Die Ausführungsbestimmungen konkretisieren den im BGEID geschaffenen Rahmen für die Bearbeitung, Aufbewahrung und Löschung von Daten.

Das BIT stellt ein öffentlich zugängliches Basisregister bereit. Es ermöglicht Verifikatorinnen zu prüfen, dass Nachweise nicht nachträglich verändert wurden und von den eingetragenen Ausstellerinnen stammen. Enthalten sind kryptografische Schlüssel zur Überprüfung der Authentizität und Integrität der Nachweise, Identifikatoren der Ausstellerinnen und Verifikatorinnen sowie Daten über deren Widerruf. Die Widerrufsdaten dürfen keine Rückschlüsse auf die Identität der Inhaberin oder den Inhalt des Nachweises zulassen.

Für die Eintragung im Basisregister sind selbstdeklarierte Angaben erforderlich. Anpassungen im Register werden täglich gespeichert und zehn Jahre lang aufbewahrt. Beim Abfragen des Registers fallen Daten wie IP-Adressen an, die zur Sicherheit und Wartung der Infrastruktur maximal 90 Tage gespeichert werden dürfen. Die Speicherung von Daten bei der Vorweisung und Überprüfung elektronischer Nachweise erfordert die Einwilligung der Inhaberin, die jederzeit widerrufen werden kann. Alle anderen Daten werden 90 Tage nach Erfassung vernichtet.

Das BIT stellt ein öffentlich zugängliches Vertrauensregister zur Verfügung. Es enthält geprüfte Informationen über die Identität von Ausstellerinnen und Verifikatorinnen, um eine sichere Nutzung elektronischer Nachweise zu gewährleisten. Die Aufnahme ins Register erfolgt nur auf Antrag und mit expliziter Einwilligung der betroffenen Person. Weitere geprüfte Daten können Handelsregister-Informationen oder Bescheinigungen sein. Zusätzliche Personendaten wie Kontaktdaten zeichnungsberechtigter Personen werden im Prüfprozess erhoben, aber nicht öffentlich zugänglich gemacht.

Das BIT stellt eine Anwendung zur Verifikation elektronischer Nachweise bereit. Damit kann auf einfache Weise die kryptografische Gültigkeit eines Nachweises überprüft werden, insbesondere der E-ID. Der Bund als Herausgeber hat keinen Zugriff auf die Inhalte der elektronischen Nachweise oder auf die Informationen bezüglich deren Verwendung. In der Anwendung können Nutzende diverse Nachweise ablegen und Personendaten dezentral speichern. Der Bund als Herausgeber der Anwendung hat keinen Zugriff auf die Inhalte der elektronischen Nachweise. Auch Sicherheitskopien, die auf einem vom Bund betriebenen System gespeichert werden, bleiben dank benutzerseitiger Verschlüsselung unlesbar. Zur Sicherstellung der digitalen Brieftaschenauthentizität werden technische Identifikatoren verwendet, die primär durch die Ausstellerin der E-ID verarbeitet werden.

Die elektronische Brieftasche ermöglicht es Nutzenden, Daten von Nachweisen verschlüsselt auf einem Sicherheitskopien-System zu speichern. Beim Abruf muss sich die Person eindeutig authentifizieren. Auch wenn diese Daten verschlüsselt sind und dem Bund nicht zugänglich bleiben, stellt die Speicherung eine Bearbeitung von Personendaten oder gegebenenfalls von besonders schützenswerten Personendaten dar. Der Zweck der Bearbeitung dient ausschliesslich der Bereitstellung eines Dienstes zur Sicherung der Nachweise gegen Verlust.

Die E-ID enthält Personendaten wie den amtlichen Namen, Vornamen, Geburtsdatum, Geschlecht, Heimatort, Geburtsort, Nationalität, Gesichtsbild und AHV-Nummer. Sie kann zusätzliche Informationen über den im Ausstellungsprozess verwendeten Ausweis enthalten. Im Informationssystem zur Ausstellung und zum Widerruf der E-ID werden auch Daten zur Ausstellung, zum Widerruf sowie zur gesetzlichen Vertretung von Minderjährigen oder Personen mit Beistand erfasst. Für die Identitätsprüfung wird eine kurze Videoaufnahme des Gesichts angefertigt, die ausschliesslich zur Untersuchung von Identitätsmissbrauch genutzt werden darf.

Das Informationssystem zur Ausstellung und zum Widerruf der E-ID speichert relevante Daten für 20 Jahre nach dem Ausstellungsdatum, Daten über den Ausstellungsprozess einschliesslich biometrischer Daten für fünf Jahre nach dem Ablaufdatum der E-ID hinaus und alle anderen Daten für 90 Tage. Die Speicherung der E-ID erfolgt dezentral auf dem Smartphone der Inhaberin. fedpol als Ausstellerin der E-ID wird nicht über die Verwendung der E-ID informiert. Die Inhaberin entscheidet selbst, welche Daten sie beim Vorweisen weitergibt. Verifikatorinnen sind gesetzlich verpflichtet, die personenbezogenen Daten zu schützen.

Vor dem Hintergrund der im Rahmen der Systeme für Sicherheitskopien, E-ID-Ausstellung und Vertrauensinfrastruktur vorgesehenen Bearbeitung personenbezogener Daten können Grundrechte betroffener Personen tangiert sein. Entsprechend erfolgt eine vertiefte Datenschutzfolgenabschätzung, um das Risiko für die Grundrechte umfassend einzuschätzen.