23.xxx

Botschaft zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise

vom ...

Sehr geehrter Herr Nationalratspräsident
Sehr geehrte Frau Ständeratspräsidentin
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise sowie des Bundesbeschlusses über die Verpflichtungskredite für den Aufbau und den Betrieb der E-ID.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

2021 M 21.3124	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)
2021 M 21.3125	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)
2021 M 21.3126	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)
2021 M 21.3127	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)
2021 M 21.3128	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)
2021 M 21.3129	Vertrauenswürdige staatliche E-ID (N 14.9.21; S 13.6.22)

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrte Frau Ständeratspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Übersicht

Mit der neuen kostenlosen und freiwilligen elektronischen Identität (E-ID) sollen sich Nutzerinnen und Nutzer künftig sicher, schnell und unkompliziert digital ausweisen können. Die E-ID soll vom Bund herausgegeben werden und den grösstmöglichen Schutz der Personendaten gewährleisten. Weiter ist vorgesehen, dass Inhaberinnen und Inhaber die grösstmögliche Kontrolle über ihre Daten haben. Die zum Zweck der E-ID geschaffene staatliche Vertrauensinfrastruktur soll auch von anderen Behörden und von Privaten genutzt werden können, die elektronische Nachweise ausstellen und verifizieren möchten.

Ausgangslage

Nach der Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste in der Volksabstimmung vom 7. März 2021 beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement, in Zusammenarbeit mit der Bundeskanzlei und dem Eidgenössischen Finanzdepartement, eine sichere staatliche elektronische Identifizierung zu entwerfen. Inzwischen haben der Nationalrat und der Ständerat sechs gleichlautende Motionen aus allen Fraktionen gutgeheissen mit dem Anliegen, ein staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität zu schaffen.

Um bereits zu einem frühen Zeitpunkt interessierte Kreise in die Erarbeitung des neuen Gesetzes einzubeziehen, hat das Bundesamt für Justiz im Herbst 2021 eine informelle öffentliche Konsultation durchgeführt. Gestützt auf die Stellungnahmen hat der Bundesrat am 17. Dezember 2021 einen Richtungsentscheid gefällt und die Grundsätze der neuen staatlichen E-ID festgelegt. Der Gesetzesentwurf wurde am 29. Juni 2022 in die Vernehmlassung geschickt, die bis am 20. Oktober 2022 dauerte.

Inhalt der Vorlage

Mit der neuen E-ID können sich Nutzerinnen und Nutzer sicher, schnell und unkompliziert digital ausweisen. Alle Personen, die über eine Schweizer Identitätskarte, einen Schweizer Pass oder einen von der Schweiz ausgestellten Ausländerausweis verfügen, können eine E-ID beantragen. Der Bund bietet eine App für das Smartphone an, in der die E-ID sicher verwaltet werden kann. Die E-ID kann sowohl im Internet – zum Beispiel bei der elektronischen Bestellung eines Strafregisterauszugs – als auch im analogen Kontext – beispielsweise als Altersnachweis beim Kauf von Alkohol – zum Einsatz kommen. Anders als bei der abgelehnten Vorlage ist der Bund für die Herausgabe der E-ID verantwortlich und betreibt die benötigte Infrastruktur.

Inhaberinnen und Inhaber einer E-ID haben grösstmögliche Kontrolle über ihre Daten (Self-Sovereign Identity). Der Datenschutz wird – wie in den Motionen gefordert – durch das System selber (privacy by design and by default), aber auch durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit) sowie eine dezentrale Datenspeicherung gewährleistet. Der Bundesrat hat das Gesetz zudem so technologieneutral wie möglich formuliert, um auf Entwicklungen reagieren zu

können. In jedem Fall hält das Schweizer E-ID-System internationale Standards ein, damit die E-ID dereinst auch im Ausland anerkannt und eingesetzt werden kann.

Die Nutzung einer E-ID ist freiwillig und kostenlos. Die Identifizierung vor Ort in einem analogen Prozess bleibt möglich, auch wenn eine E-ID zum Einsatz kommen kann. Gleichzeitig müssen alle Behörden, auch jene der Kantone und Gemeinden, die E-ID akzeptieren, wenn sie eine elektronische Identifizierung vornehmen, so zum Beispiel bei der Ausstellung einer Wohnsitzbestätigung oder eines Betreibungsregisterauszugs.

Die zum Zweck der E-ID geschaffene staatliche Vertrauensinfrastruktur soll auch von den kantonalen und kommunalen Behörden und von Privaten genutzt werden können, die elektronische Nachweise ausstellen möchten. So sollen amtliche Dokumente wie Wohnsitzbestätigungen oder Betreibungsregisterauszüge, aber auch Diplome, Tickets oder Mitgliederausweise mit der geplanten staatlichen Vertrauensinfrastruktur ebenfalls als digitale Nachweise herausgegeben und in der vom Bund zur Verfügung gestellten oder einer anderen von ihm gewählten Applikation sicher verwaltet werden können.

Gleichzeitig mit dem Gesetz wird dem Parlament ein Bundesbeschluss über die Verpflichtungskredite für den Aufbau und den Betrieb der E-ID vorgelegt. Beantragt werden ein Zusatzkredit im Umfang von 15,3 Millionen Franken sowie zwei weitere Verpflichtungskredite für insgesamt 85,1 Millionen Franken.

Inhaltsverzeichnis

Botschaft

1 Ausgangslage

Am 7. März 2021 wurde das Bundesgesetz über elektronische Identifizierungsdienste an der Urne mit 64 Prozent Nein-Stimmen abgelehnt. Am 10. März 2021 sind sechs inhaltlich identische Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» von allen Fraktionen eingereicht worden (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129). Zudem wurden innerhalb von drei Monaten nach der Abstimmung die Interpellation 21.3310 Andrey «Identitätskarte als Teil einer zukünftigen E-ID-Lösung» und die Interpellation 21.3718 Graf-Litscher «Selbstbestimmte elektronische Identitäten» eingereicht. Die sechs Motionen wurden vom Nationalrat am 14. September 2021 und vom Ständerat am 13. Juni 2022 angenommen. Die Diskussion zur Interpellation 21.3310 Andrey wurde verschoben und am 17 März 2023 wurde die Interpellation abgeschrieben. Zudem hat der Nationalrat beschlossen, die Interpellation 21.3718 Graf-Litscher zu erledigen.

An seiner Sitzung vom 26. Mai 2021 erklärte der Bundesrat, dass er rasch eine neue Lösung für den elektronischen Identitätsnachweis vorlegen wolle, der den Anliegen der Motionen Rechnung trägt. Er hat daher das EJPD beauftragt, bis Ende 2021 zusammen mit dem Eidgenössischen Finanzdepartement (EFD) und der Bundeskanzlei (BK) und in enger Absprache mit den Kantonen und den beiden Eidgenössischen Technischen Hochschulen Zürich und Lausanne einen Textentwurf zu erarbeiten. Es ging insbesondere darum, die verschiedenen technischen Lösungsansätze für die E-ID zu prüfen und die jeweiligen Aufwände zu beziffern.

Das EJPD hat zum Projekt der elektronischen Identität (E-ID) unter Einbezug der Kantone und der Wissenschaft ein Papier[1] erarbeitet (im Folgenden «Diskussionspapier»). Diese Auslegeordnung enthält verschiedene Begriffsbestimmungen der E-ID und der entsprechenden Vertrauensinfrastruktur. Zudem werden drei technische Lösungsansätze präsentiert: Self-Sovereign Identity (SSI), Public-Key-Infrastruktur (PKI) und zentraler staatlicher Identitätsprovider (IdP). Die Auslegeordnung legt insbesondere auch deren Einbettung in das wirtschaftliche und gesellschaftliche Umfeld dar und beleuchtet verschiedene Einsatzmöglichkeiten einer staatlichen E-ID.

Vom 2. September bis am 14. Oktober 2021 fand dazu eine informelle öffentliche Konsultation statt. Es gingen sechzig Stellungnahmen von kantonalen Verwaltungen sowie von Vertreterinnen und Vertretern aus Wissenschaft, Wirtschaftsorganisationen und Firmen ein.[2] Am 14. Oktober 2021 organisierte das EJPD zum Abschluss der Konsultation eine Konferenz mit einer öffentlichen Diskussion, an der fünfzig Vertreterinnen und Vertreter von Kantonen, Politik, Wissenschaft, Zivilgesellschaft und Wirtschaft sowie interessierte Privatpersonen teilnahmen. Die informelle öffentliche Konsultation hatte zum Ziel, die Meinungen zu den wichtigsten Anforderungen an

1 www.bj.admin.ch > Staat & Bürger > Laufende Rechtsetzungsprojekte > Staatliche e-ID > Öffentliche Konsultation zum «Zielbild E-ID»

2 www.bj.admin.ch > Staat & Bürger > Laufende Rechtsetzungsprojekte > Staatliche E-ID > Übersicht über das Ergebnis der öffentlichen Konsultation zum «Zielbild E-ID»

eine E-ID, den wichtigsten Einsatzbereichen und den erwarteten Vorteilen zusammenzutragen. Zudem ging es darum, die Meinungen der interessierten Personen zum Umfang des E-ID-Ökosystems in Erfahrung zu bringen. Die zusammengetragenen Informationen erlaubten es dem Bundesrat, einen Grundsatzentscheid für die neue Stossrichtung der E-ID zu treffen.

Die Konsultationsteilnehmenden sprachen sich für einen SSI-Ansatz aus. Sie waren zudem der Ansicht, dass eine Vertrauensinfrastruktur mit einem Ambitionsniveau 3 (vgl. Diskussionspapier Kap. 4.2) erforderlich ist. Dieses Vorgehen steht im Einklang mit den Forderungen der sechs Motionen, die nach der Abstimmung eingereicht wurden. Im Rahmen der künftigen Arbeiten ist es angezeigt, diesem Willen sowie den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung Rechnung zu tragen. Zudem möchte das EJPD enger mit den Ämtern und Kantonen zusammenarbeiten, die in diesem Bereich entsprechende Pilotprojekte durchführen.

Gestützt auf die Ergebnisse der informellen öffentlichen Konsultation hat der Bundesrat am 17. Dezember 2021 über die neue Stossrichtung der E-ID entschieden. Demnach soll die E-ID-Vorlage einen Ansatz verfolgen, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik, der Datensparsamkeit und der dezentralen Datenspeicherung sowie auf einer staatlichen Vertrauensinfrastruktur beruht, mit der ein Ökosystem für elektronische Nachweise eingeführt werden kann, die von Akteuren des öffentlichen und des privaten Sektors ausgestellt werden. Dem EJPD wurde, in Zusammenarbeit mit dem EFD (Digitale Verwaltung Schweiz DVS) und der BK (Digitale Transformation und IKT-Lenkung DTI), die Verantwortung für die Sicherstellung des Informationsflusses und für die Koordination der Abhängigkeiten zwischen dem Vorentwurf und verwandten Projekten von Bund und Kantonen übertragen.

Der Vorentwurf wurde am 29. Juni 2022 in die Vernehmlassung geschickt, die bis am 20. Oktober 2022 dauerte. Insgesamt gingen 117 Stellungnahmen ein, wobei die Mehrheit den Vorentwurf begrüsste. Insbesondere fand die neue Rollenverteilung, in der der Staat als Herausgeber der elektronischen Identität und als Betreiber der erforderlichen Vertrauensinfrastruktur agiert, breite Zustimmung. Es besteht insgesamt der klare Wunsch, dass rasch eine stabile, sichere und benutzerfreundliche Lösung zur Verfügung steht. Gestützt auf die Vernehmlassungsergebnisse hat der Bundesrat diesen Gesetzesentwurf erarbeitet.

1.1 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage eines Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) ist in der Botschaft vom 27. Januar 2016 zur Legislaturplanung 2015–2019[3] und im Bundesbeschluss vom 14. Juni 2016[4] über die Legislaturplanung 2015–2019 angekündigt. Nach der Ablehnung dieser Vorlage in der Abstimmung

3 BBl **2016** 1105, 1171 und 1222
4 BBl **2016** 5183, hier 5184–5185

vom 7. März 2021 entschied der Bundesrat, die Gesetzgebungsarbeiten im Bereich der E-ID wieder aufzunehmen und neu auszurichten. Angesichts der unerwarteten Situation wurde die Vorlage weder in der Botschaft vom 29. Januar 2020 zur Legislaturplanung 2019–2023[5] noch im Bundesbeschluss vom 21. September 2020 über die Legislaturperiode 2019–2023[6] angekündigt.

1.2 Erledigung parlamentarischer Vorstösse

Dieser Gesetzesentwurf setzt die folgenden parlamentarischen Vorstösse um:

- Motionen aller Fraktionen 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129 «Vertrauenswürdige staatliche E-ID». Die Motionen verlangen, dass der Staat ein elektronisches Identifikationsmittel zum Nachweis der eigenen Identität (Authentifizierung) in der virtuellen Welt, vergleichbar mit Identitätskarte oder Pass in der physischen Welt, schafft. Dabei sollen insbesondere die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) eingehalten werden. Diese Motionen wurden im Nationalrat am 14. September 2021 und im Ständerat am 13. Juni 2022 gemäss dem Antrag des Bundesrates verabschiedet.

Bei der Erarbeitung der Vorlage wurde auch folgenden parlamentarischen Vorstössen Rechnung getragen:

- Interpellation 21.3310 Andrey «Identitätskarte als Teil einer zukünftigen E-ID-Lösung». Der Bundesrat hat am 26. Mai 2021 die Fragen der Interpellation beantwortet. Am 17. März 2023 wurde die Interpellation abgeschrieben, weil sie im Nationalrat nicht innert zwei Jahren abschliessend behandelt worden war.

- Interpellation Graf-Litscher 21.3718 «Selbstbestimmte elektronische Identitäten». Am 18. August 2021 hat der Bundesrat die Fragen beantwortet. Am 1. Oktober 2021 hat der Nationalrat beschlossen, die Interpellation zu erledigen.

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

2.1 Erstes E-ID-Gesetz

Die Arbeiten am ersten E-ID-Gesetz wurden 2013 aufgenommen. Das Parlament verabschiedete am 27. September 2019 mit deutlichem Mehr das Bundesgesetz über

5 BBl **2020** 1777
6 BBl **2020** 8385

elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID). Dieses sah vor, dass vornehmlich private Identityprovider anhand der vom Bundesamt für Polizei (fedpol) zur Verfügung gestellten Daten die E-ID ausstellen würden. Der Bund wäre nur als Ausstellerin von E-ID aktiv geworden, hätten sich dafür keine anderen Austellerinnen finden lassen. Dagegen wurde erfolgreich das Referendum ergriffen. Das E-ID-Gesetz wurde in der Volksabstimmung vom 7. März 2021 deutlich abgelehnt. Die Vox-Analyse zum Abstimmungsergebnis zeigte allerdings, dass die Mehrheit der Stimmenden sich nicht per se gegen einen E-ID ausgesprochen hat, sondern gegen eine E-ID von privaten Anbieterinnen.

2.2 Diskussionspapier zum Zielbild E-ID

Nach der Ablehnung des E-ID-Gesetzes wurden am 10. März 2021 sechs Motionen mit identischem Wortlaut eingereicht: (siehe dazu Kapitel 1.2). Die Motionen gaben zwar die grundsätzlichen Ziele für die künftige Ausgestaltung einer E-ID vor, nicht aber mit welcher E-ID-Konzeption diese erreicht werden soll. Da der Vernehmlassungsprozess eher ungeeignet ist, einen Variantenentscheid zur grundsätzlichen Ausrichtung einer Vorlage herbeizuführen, wurde am 2. September 2021 die öffentliche Konsultation zum Diskussionspapier zum Zielbild E-ID im Rahmen eines Beiratstreffens unter der Leitung der Departmentsvorsteherin eröffnet.

Das zur Konsultation vorgelegte Diskussionspapier zum Zielbild E-ID stellt eine Auslegeordnung dar. Es stellt mögliche Definitionen und Dimensionen für eine zukünftige Schweizer E-ID und der damit verbundenen Infrastruktur in den Raum und breitet drei technische Lösungsansätze aus:

- Self-Sovereign Identity (SSI)
- Public-Key-Infrastruktur (PKI)
- zentraler staatlicher Identitätsprovider (IdP)

Eine Mehrheit der Teilnehmenden an der öffentlichen Konsultation sprach sich hinsichtlich des Technologieansatzes für SSI als den bestmöglichen zur Erfüllung der geforderten Werteversprechen und Funktionen aus. Minderheiten votierten für die Varianten PKI beziehungsweise IdP, hauptsächlich da diese Ansätze lang erprobt sind.

Zum Sicherheitsaspekt, ob bei der Umsetzung auf ein Hard-Token (physisches Gerät/Element zur Aufbewahrung von digitalen privaten Schlüsseln) zurückgegriffen werden soll, sprach sich eine Mehrheit gegen ein Hard-Token und zugunsten der Benutzerfreundlichkeit ohne Hard-Token aus. Aus Sicht einiger weniger Stellungnahmen führte für eine sichere E-ID kaum ein Weg an einem physischen Token vorbei. Neben dem Technologieansatz wurde im Zielbild E-ID zudem in Anlehnung an die Diskussionen in der europäischen Union (EU) die Ambitionsniveaus zur Diskussion gestellt:

- Ambitionsniveau 1: Die E-ID bleibt der einzig verfügbare digitale Nachweis.
- Ambitionsniveau 2: Neben der E-ID kann der Staat auch andere digitale Nachweise ausstellen.

- Ambitionsniveau 3: Nicht nur der Staat, sondern auch Private können andere digitale Nachweise ausstellen.

Das Ambitionsniveau 3 als Zielgrösse wurde von fast allen Teilnehmenden genannt, welche sich explizit zum Ambitionsniveau geäussert haben. Allerdings war ein schrittweiser Ausbau – von Ambitionsniveau 1 auf 2 und schlussendlich auf 3 –für einige Teilnehmende durchaus denkbar. Mit einer öffentlichen konferenziellen Diskussion am 14. Oktober 2021 wurde die Konsultation abgeschlossen.

2.3 Richtungsentscheid des Bundesrats

Basierend auf den Ergebnissen der Konsultation zum Zielbild E-ID legte der Bundesrat am 17. Dezember 2021 die Grundsätze für die Ausgestaltung einer künftigen staatlichen E-ID fest: Nutzerinnen und Nutzer der E-ID sollen grösstmögliche Kontrolle über ihre Daten haben (Self-Sovereign Identity). Der Datenschutz soll unter anderem durch das System selber (privacy by design), aber auch durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit) sowie eine dezentrale Datenspeicherung gewährleistet werden. Die E-ID soll auf einer staatlich betriebenen Infrastruktur beruhen. Sie könnte staatlichen und privaten Stellen für die Ausstellung unterschiedlicher digitaler Nachweise zur Verfügung stehen (E-ID-Ökosystem mit Ambitionsniveau 3).

2.4 Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens

Vom 29. Juni bis 20. Oktober 2022 fand die Vernehmlassung zum (zweiten) E-ID-Gesetz statt. Insgesamt gingen 117 Stellungnahmen ein.

2.4.1 Allgemeine Anmerkungen

Die Rückmeldungen zum neuen Gesetzesvorentwurf sind überwiegend positiv. Insbesondere findet die neue Rollenverteilung, in welcher der Staat als Herausgeber der elektronischen Identität und als Betreiber der erforderlichen Vertrauensinfrastruktur agiert, breite Zustimmung. Es besteht insgesamt der klare Wunsch, dass rasch eine stabile, sichere und benutzerfreundliche Lösung zur Verfügung steht. Ebenfalls begrüsst werden die Geschwindigkeit in der Erarbeitung des Gesetzesvorentwurfs und das partizipative, transparente Vorgehen.
In drei Stellungnahmen wird der Gesetzesvorentwurf grundsätzlich abgelehnt: Die SVP stellt die verfassungsrechtliche Grundlage in Frage. Der Datenschützer des Kantons Tessin sowie die Piratenpartei lehnen die Vorlage aus Gründen des Datenschutzes ab; die Piratenpartei macht zusätzliche Gründe geltend.

2.4.2 Bemerkungen zum Konzept der selbstbestimmten elektronischen Identität und der Rolle des Staates

In den Stellungnahmen wird die Rolle des Staates – anders als beim abgelehnten ersten E-ID-Gesetz mit Privaten als Herausgeberinnen der elektronischen Identitäten –

nur noch am Rande thematisiert. Es ist unbestritten, dass der Staat die tragende Rolle bei der Entwicklung und dem Betrieb der Vertrauensinfrastruktur spielen und der einzige Herausgeber der staatlichen elektronischen Identität sein soll.
Die Vorzüge des Konzepts der selbstbestimmten elektronischen Identität werden anerkannt, ermöglicht es doch eine Umsetzung der Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung. Gleichzeitig stösst auf Anklang, dass die Nutzung der Vertrauensinfrastruktur auch Privaten möglich sein soll.

2.4.3 Einzelfragen

Im Rahmen der Vernehmlassung wurden insbesondere folgende Einzelfragen kontrovers verhandelt:

- Hinsichtlich des Kreises der zur Beantragung einer E-ID berechtigten Personen wird von verschiedener Seite gefordert, diesen Kreis zu erweitern. Andererseits wird gefordert, diesen Kreis einzuschränken, um sicherzustellen, dass nur jenen Personen eine E-ID ausgestellt wird, deren Identität verlässlich festgestellt werden kann.
- Mit Blick auf den Ausstellungsprozess der E-ID wurde eine Vielzahl von Forderungen eingereicht. Neben verschiedenen Detailfragen ist insbesondere die Forderung zu nennen, zusätzlich zum Online-Ausstellungsprozess auch die Ausstellung am Schalter vorzusehen.
- Naturgemäss ist das Thema Datenschutz in den meisten Stellungnahmen ein zentrales Thema. Viele sprechen sich für einen höheren Datenschutz aus, insbesondere was mögliche Überidentifikationen betrifft. Mit Überidentifikation ist das Verlangen der E-ID ohne rechtmässigen Grund oder das Verlangen von mehr als den minimal erforderlichen Bestandteilen der E-ID gemeint.
- Der Gesetzesvorentwurf macht zur Frage der Barrierefreiheit keine Aussagen, weil der Bund dazu per Gesetz immer verpflichtet ist. Dessen ungeachtet liegt eine Vielzahl von Forderungen vor, diesen Aspekt im E-ID-Gesetz ausdrücklich zu regeln.
- Der Gesetzesvorentwurf sieht vor, dass die Kantone Anlaufstellen bezeichnen, die im Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten. Während der Bedarf an Support unbestritten ist, wird der Bund in vielen Stellungnahmen stärker in Pflicht genommen und gefordert, dass er einen zentralen Helpdesk betreibt. Die Kantone sehen sich vor allem für Hilfestellungen im Zusammenhang der Nutzung der E-ID im E-Government verantwortlich.

2.5 Würdigung der Ergebnisse des Vernehmlassungsverfahrens

Entgegen der Argumentation der SVP ist der Bundesrat der Meinung, dass das E-ID-Gesetz auf einer soliden verfassungsmässigen Grundlage basiert (vgl. dazu Kapitel 7.1). Die Bedenken hinsichtlich des Datenschutzes seitens des Datenschützers des

Kantons Tessin und der Piratenpartei sind im Grundsatz zwar nachvollziehbar, aber rechtfertigen nicht die Ablehnung des Gesetzvorentwurfs (vgl. dazu Kapitel 7.7).

Von den in der Vernehmlassung formulierten Forderungen sind insbesondere folgende im Gesetzesentwurf aufgenommen worden:

- Neben dem Online-Ausstellungsprozess wird neu auch eine Ausstellung vor Ort möglich.
- Restriktionen zur Verhinderung von Abfragen von E-ID-Daten, welche für die gewünschte Dienstleistung nicht notwendig sind, und Sanktion sind vorgesehen.
- Die Zugänglichkeit für Menschen mit Behinderung wird explizit geregelt.
- Nachdem im Gesetzesvorentwurf vorgesehen war, dass die Kantone Anlaufstellen zur Unterstützung anbieten, schlägt nun der Gesetzesentwurf vor, dass fedpol und das Bundesamt für Informatik und Telekommunikation (BIT) den Nutzerinnen und Nutzern bei der Ausstellung der E-ID und der Nutzung der Vertrauensinfrastruktur einen Support zur Verfügung stellen.

3 Rechtsvergleich, insbesondere mit dem europäischen Recht

In der EU sind im Bereich der E-ID Reformen im Gange. Der Bundesrat ist der Ansicht, dass diese Entwicklungen in die Überlegungen auf nationaler Ebene einbezogen werden sollten. Am 3. Juli 2021 verabschiedete die Europäische Kommission einen Vorschlag[7] zur Änderung der Verordnung (EU) Nr. 910/2014[8] (eIDAS-Verordnung) und zur Schaffung eines rechtlichen Rahmens für eine europäische digitale Identität. Im Rahmen dieser neuen Verordnung ist vorgesehen, dass die Mitgliedstaaten den Bürgerinnen und Bürgern sowie Unternehmen innerhalb von 12 Monaten nach dem Inkrafttreten elektronische Brieftaschen zur Verfügung stellen, in denen diese ihre nationale elektronische Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerschein, Abschlusszeugnisse, Bankkonto) verknüpfen können. Die Brieftaschen können von Behörden oder privaten Einrichtungen bereitgestellt werden, sofern diese von den Mitgliedstaaten anerkannt sind.

Am 6. Dezember 2022 hat der Rat seine allgemeine Ausrichtung für die europäische digitale Identität festgelegt. Im Europäischen Parlament wurde der Ausschuss Industrie, Forschung und Energie (ITRE) mit dem Vorschlag betraut. Das Parlament hat seinen Standpunkt am 16. März 2023 festgelegt und anschliessend wurden die Verhandlungen aufgenommen. Damit der Vorschlag in nützlicher Frist umgesetzt werden kann, wird er durch eine Empfehlung ergänzt. Die Kommission forderte die Mitgliedstaaten auf, ein gemeinsames Instrumentarium zu schaffen und unverzüglich mit den erforderlichen Vorarbeiten zu beginnen. Dieses Instrumentarium wird die technische Architektur, Normen, Leitlinien und bewährte Verfahren umfassen. Am

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM (2021) final, 3. Juni 2021.

8 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73.

10. Februar 2023 veröffentlichte die Kommission ihre erste Version eines gemeinsamen EU-Instrumentariums für die Einführung einer elektronischen Brieftasche für die europäische digitale Identität (EUid-Brieftasche)[9].

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. Die Mitgliedstaaten verhandeln untereinander die technischen Standards seit September 2021.

Die Schweiz ist rechtlich nicht verpflichtet, die E-IDAS-Verordnung und die dazu gehörenden Änderungen 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. Der Gesetzesentwurf sieht vor, dass der Bundesrat internationale Abkommen abschliessen kann, um eine internationale Anerkennung der E-ID zu erreichen und ausländische E-ID zu anerkennen (Art. 31). So wird es möglich sein, eine gegenseitige Anerkennung, insbesondere mit der EU, zu erlangen. Der Gesetzesentwurf wurde so formuliert, dass er mit dem europäischen Recht vereinbar ist.

4 Grundzüge der Vorlage

4.1 Beantragte Regelung

Der Gesetzesentwurf sieht für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises die Einführung eines kostenlosen und freiwilligen staatlichen elektronischen Identitätsnachweises vor. Dabei nimmt der Staat weiterhin seine zentrale Aufgabe der Überprüfung der Identität einer Person und der Ausstellung des entsprechenden elektronischen Nachweises wahr. Wie in den im Nationalrat eingereichten Motionen gefordert, verfolgt die neue Vorlage einen Ansatz, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik und datenschutzfreundliche Voreinstellungen, der Datensparsamkeit und der dezentralen Datenspeicherung beruht.

Zudem sieht der Gesetzesentwurf die Schaffung einer staatlichen Vertrauensinfrastruktur vor, die es Akteuren des öffentlichen und privaten Sektors ermöglicht, elektronische Nachweise auszustellen und zu verwenden. Der Staat wird das erforderliche Basissystem betreiben (Basisregister, Vertrauensregister) und eine staatliche elektronische Brieftasche in Form einer mobilen Anwendung zur Verfügung stellen, die die E-ID und weitere elektronische Nachweise enthalten kann. Inhaberinnen und Inhaber der Brieftasche können damit ihre E-ID und andere elektronische Nachweise sicher und transparent vorweisen. Mit einer solchen Öffnung des Systems kann die Verbreitung der elektronischen Nachweise verbessert und ihre Nutzung erhöht werden. Gleichzeitig kann so das Vertrauen der Bevölkerung in die elektronischen Prozesse gestärkt werden. Alternative Anwendungen für die Aufbewahrung und Vorweisung

9 The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework: the Digital Identity Wallet Architecture and Reference Framework, Januar 2023, Version 1.0.0.

elektronischer Nachweise (elektronische Brieftasche) können verwendet werden, sofern sie technisch kompatibel sind.

Die Einführung einer elektronischen Vertrauensinfrastruktur durch den Staat ist eine wichtige und neue Entwicklung. Zudem basiert diese Vorlage auf einem neuartigen partizipativen Verfahren, das eine informelle Konsultation, öffentliche Diskussionen und ein Online-Forum für fachliche Diskussionen umfasst. Auch Erfahrungen aus Pilotprojekten mit anderen Ämtern und der Austausch mit anderen Ländern fliessen in die Vorlage ein.

Die Frage der Verwendung der E-ID in verschiedenen Bereichen ist im Gesetzesentwurf nur exemplarisch geregelt (vgl. Änderungen anderer Erlasse: Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs [SchKG][10] und Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier [EPDG][11]). Dieser Punkt wurde im Rahmen der Vernehmlassung thematisiert. Angesichts der Einsatzvielfalt sollte die Verwendung der E-ID in den für die jeweiligen Bereiche geltenden Gesetzen geregelt werden.

4.2 Abstimmung von Aufgaben und Finanzen

Eine Schätzung der Aufwände wurde vorgenommen (vgl. Kap. 6.1 Finanzielle und personelle Auswirkungen auf den Bund).

Insgesamt werden im Zeitraum 2023 bis 2028 für die Entwicklung und den Betrieb der Vertrauensinfrastruktur, die Ausgabe der E-ID und die Pilotprojekte rund 181,9 Millionen Franken benötigt. Ab 2029 ist mit Aufwänden von rund 24,7 Millionen Franken pro Jahr zu rechnen.

Dieser Mittelbedarf darf für ein Projekt mit dieser Bedeutung und als Grundlage für das Voranbringen der Digitalisierung in der Schweiz als angemessen bezeichnet werden.

4.3 Umsetzung

Die Ausführungsbestimmungen für die Umsetzung dieses Gesetzes werden auf Verordnungsstufe geregelt (vgl. Art. 28 und entsprechende Erläuterungen).

5 Erläuterungen zu den einzelnen Artikeln

Ingress

Der Gesetzesentwurf stützt sich auf die Artikel 38 Absatz 1, 81 und 121 Absatz 1 der Bundesverfassung[12] (BV).

10 SR **281.1**
11 SR **816.1**
12 SR **101**

Was die staatliche elektronische Identität angeht, stützt sich der Vorentwurf auf Artikel 38 Absatz 1 und 121 Absatz 1 BV. Gemäss Artikel 38 Absatz 1 BV ist der Bund dafür zuständig, Erwerb und Verlust der Bürgerrechte durch Abstammung, Heirat und Adoption zu regeln. Gemäss Artikel 121 Absatz 1 BV ist die Gesetzgebung über die Ein- und Ausreise, den Aufenthalt und die Niederlassung von Ausländerinnen und Ausländern sowie über die Gewährung von Asyl Sache des Bundes. Obwohl die beiden Artikel nicht ausdrücklich die Ausweise regeln, lässt sich daraus die Kompetenz des Bundes ableiten, die erforderlichen Ausweise zu regeln. Dies selbst dann, wenn diese nicht ausschliesslich dem Nachweis der Staatsangehörigkeit der Schweizer Bürgerinnen und Bürger und des Aufenthaltsstatus der Ausländerinnen und Ausländer dienen. Gestützt auf diese beiden Artikel ermächtigen das Ausweisgesetz vom 22. Juni 2001[13] (AwG) und das Ausländer- und Integrationsgesetz vom 16. Dezember 2005[14] (AIG) den Bund, den Schweizer Bürgerinnen und Bürgern Identitätsausweise und den Ausländerinnen und Ausländern Ausländerausweise auszustellen. Da die staatliche E-ID zum Nachweis der Identität in der virtuellen Welt dient und das Recht, eine E-ID zu erhalten, eng mit dem Recht verknüpft ist, den entsprechenden Ausweis als physisches Dokument zu beziehen, ist es gerechtfertigt, diesen Gesetzesentwurf für den amtlichen Nachweis der Identität, der Staatsangehörigkeit und des Aufenthaltsstatus der Ausländerinnen und Ausländer auf die gleiche Verfassungsgrundlage zu stützen.

Die Kompetenz zur Schaffung einer Vertrauensinfrastruktur für die E-ID ergibt sich aus Artikel 81 BV, gemäss dem der Bund im Interesse des ganzen oder eines grossen Teils des Landes öffentliche Werke errichten und betreiben oder ihre Errichtung unterstützen kann. Die Unterstützung für den Betrieb und den Unterhalt von Werken Dritter kann sich hingegen nicht auf Artikel 81 stützen; sie könnte sich jedoch auf eine andere Bundeskompetenz stützen. Ein «öffentliches Werk» nach dieser Bestimmung ist herkömmlicherweise physischer Art, im Sinne eines Bauwerks, wie beispielsweise ein Tunnel. Dem Rechtsgutachten des Bundesamtes für Justiz (BJ) für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen[15] zufolge wäre es nach einem in der Lehre teilweise befürworteten Ansatz jedoch möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Artikel 81 BV zu subsumieren»[16]. Gemäss der zeitgemässen und teleologischen Auslegung von Lendi[17] und von Biaggini[18] können «öffentliche Werke» auch immateriell oder nicht fest sein, wie ein im Interesse der Schweiz entwickeltes Informatik- oder Kommunikationssystem. Der

13 SR **143.1**
14 SR **142.20**
15 EJPD, Bundesamt für Justiz, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, VPB 2012.1 (S. 1–17), Ausgabe vom 1. Mai 2012.
16 Ibid., S. 8: «Zusammengefasst wäre es nach einem in der Lehre teilweise befürworteten Ansatz möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Art. 81 BV zu subsumieren».
17 Ibid.; Lendi, Martin, in St. Galler Kommentar, 2. Aufl. 2008, Art. 81 Rz. 6; Vogel, Stefan, in St. Galler Kommentar, 4. Aufl. 2023, Art. 81 N 5.
18 Ibid.; Biaggini, Giovanni, in BV-Kommentar, Zürich 2007, Art. 81 Rz. 2, kritisiert von Markus Kern im Basler Kommentar, Rz. 6 und 9.

Bundesrat schliesst sich dieser Lehrmeinung an und hält es daher für zulässig, Artikel 81 BV als Grundlage für einen Gesetzesentwurf zur Schaffung einer Vertrauensinfrastruktur heranzuziehen, mit der unterschiedliche elektronische Nachweise (einschliesslich der E-ID) ausgestellt, verwendet und bestätigt werden können. In diesem Zusammenhang ist darauf hinzuweisen, dass Artikel 81 BV dem Bund nicht die Kompetenz verleiht, für die IKT-Zusammenarbeit zwischen Bund und Kantonen verbindliche technische und organisatorische Standards zu erlassen und durchzusetzen.[19] Hingegen kann der Bund die Regeln aufstellen, die für eine sichere, effiziente und einheitliche Bereitstellung und Verwendung der in Frage stehenden öffentlichen Werke notwendig sind.

Der vorliegende Gesetzesentwurf regelt bestimmte zivilrechtliche Aspekte im Zusammenhang mit den Beziehungen zwischen den Ausstellerinnen und den Inhaberinnen und Inhabern einer E-ID sowie den Verifikatorinnen und den Inhaberinnen und Inhabern einer E-ID. Angesichts deren untergeordneter Bedeutung wird im Ingress Artikel 122 Absatz 1 BV nicht erwähnt, der die Kompetenz des Bundes in zivilrechtlicher Hinsicht begründet.

1. Abschnitt Gegenstand und Zweck

Art. 1

Abs. 1

Bst. a

Der Gesetzesentwurf regelt die Anforderungen, die die Vertrauensinfrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen erfüllen muss.

Bst. b

Der Gesetzesentwurf regelt die Rollen und Verantwortlichkeiten bei der Bereitstellung und der Verwendung der Vertrauensinfrastruktur.

Bst. c

Der Gesetzesentwurf stellt den rechtlichen Rahmen für elektronische Nachweise in der Schweiz auf, einschliesslich der staatlichen elektronischen Identität.

Abs. 2

Bst. a

Der Wortlaut dieses Buchstabens wurde angepasst, um den Vernehmlassungsergebnissen Rechnung zu tragen. Mehrere Teilnehmende kritisierten, dass der Grundsatz des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen nach

19 Ibid.; Biaggini, G., ibid., Art. 81 Rz. 3.

Artikel 7 des Bundesgesetzes vom 25. September 2020[20] über den Datenschutz (DSG) in der Bestimmung nur teilweise enthalten war. Neu stützt sich dieser Buchstabe nicht mehr auf den eher allgemeinen Grundsatz nach Artikel 1 DSG, sondern auf Artikel 7 Absatz 2 DSG. Damit soll gewährleistet werden, dass die vorgesehenen technischen und organisatorischen Massnahmen, insbesondere im Hinblick auf den Stand der Technik, geeignet sind, um die Art und das Ausmass der Datenbearbeitung und das damit verbundene Risiko für den Schutz der Persönlichkeit und die Grundrechte der betroffenen Personen zu minimieren.

Dieses Ziel wird insbesondere durch die Umsetzung der Anforderungen der sechs inhaltlich identischen Motionen «Vertrauenswürdige staatliche E-ID» (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129) erreicht, die nach der Ablehnung der früheren Vorlage in der Abstimmung vom 7. März 2021 von Parlamentarierinnen und Parlamentariern aller Fraktionen eingereicht wurden. Gemäss den Motionärinnen und Motionären muss der staatliche elektronische Identitätsnachweis insbesondere den Grundsätzen «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) entsprechen. In diesem Buchstaben werden diese Anforderungen als spezifische Zwecke formuliert, die im Zusammenhang mit dem Schutz der Personendaten umgesetzt werden müssen.

Das DSG gilt für die Bearbeitung der Personendaten, die im Rahmen der Umsetzung des Gesetzes durchgeführt wird. Um Wiederholungen zu vermeiden und das Verständnis zu erleichtern, verweisen die Bestimmungen des Gesetzesentwurfs nicht auf die einschlägigen Artikel des DSG (vgl. Kap. 7.8 Datenschutz).

Darüber hinaus gilt für die Nutzung der Vertrauensinfrastruktur durch die kantonalen Behörden grundsätzlich das kantonale Datenschutzrecht, sofern die Datenbearbeitung durch die kantonalen Behörden erfolgt. Das ist insbesondere der Fall, wenn sie eigene elektronische Nachweise ausstellen oder elektronische Nachweise (einschliesslich der E-ID) überprüfen. Einige Bestimmungen des vorliegenden Gesetzes greifen allerdings punktuell in das kantonale Recht ein, das etwa die im Gesetzesentwurf vorgesehenen (höheren) Mindeststandards gleichermassen einhalten muss wie die privaten Nutzerinnen und Nutzer der Vertrauensinfrastruktur.

Bst. b

Dieser Buchstaben legt fest, dass mit dem Gesetz die Ausstellung und die Verwendung elektronischer Nachweise für eine spezifische Personengruppe ermöglicht werden sollen. Diese elektronischen Nachweise können somit ausgestellt und in Beziehungen unter Privaten und mit Behörden verwendet werden.

Mit dem Gesetzesentwurf soll die Einführung sicherer Prozesse im Rahmen der Vertrauensinfrastruktur sichergestellt werden. Die Risiken im Zusammenhang mit der Ausstellung, der Verwendung und dem Vorweisen der elektronischen Nachweise müssen über geeignete technische und organisatorische Massnahmen minimiert werden.

Bst. c

20 SR **235.1**

Mit diesem Buchstaben soll sichergestellt werden, dass die Ausgestaltung der E-ID und der Vertrauensinfrastruktur dem aktuellen Stand der Technik entspricht. Der Begriff «aktueller Stand der Technik» unterscheidet sich konzeptuell von anderen ähnlichen Begriffen wie den «anerkannten Regeln der Technik» und dem «aktuellen Stand der Wissenschaft und der Forschung». Einfach ausgedrückt, verweist der Begriff «aktueller Stand der Technik» auf innovativere Methoden als der Begriff «anerkannte Regeln der Technik» und auf ältere Methoden als der Begriff «Stand der Wissenschaft und der Forschung». Diese Unterscheidung ist bei der Bestimmung des erforderlichen Sicherheitsniveaus wesentlich. Nach Artikel 7 Absatz 2 DSG müssen ebenfalls Massnahmen ergriffen werden, die dem «Stand der Technik» entsprechen, doch es werden keine Kriterien aufgestellt, die Aufschluss über den Inhalt des Begriffs «Stand der Technik» geben. Daraus darf jedoch nicht geschlossen werden, dass das, was im Gesetz nicht konkret bestimmt ist, nicht überprüft und folglich nicht angewendet werden kann.

Der Gesetzgeber strebt mit diesem Begriff ein hohes Niveau der Datensicherheit und des Datenschutzes dank fortschrittlichen Verfahren an. Zu diesem Zweck ist die regelmässige Überprüfung der umgesetzten Sicherheitsmassnahmen auf ihre Wirksamkeit hinsichtlich der geforderten Schutzziele, ihrer Aktualität sowie ihres Innovationsgrads zu fördern. So sind die Sicherheitsmassnahmen auch mit den Sicherheitsprodukten auf dem Markt zu vergleichen. Was heute als «Stand der Technik» gilt, kann morgen aufgrund der innovationsbedingten Verschiebung, also der Alterung der Sicherheitsmassnahme, im Vergleich mit anderen verfügbaren Sicherheitsmassnahmen eher den «anerkannten Regeln der Technik» zugeordnet werden.

Bst. d

Mit dem Gesetzesentwurf soll auch die Sicherheit der Infrastruktur und der Prozesse zur Ausstellung und Überprüfung anderer elektronischer Nachweise gewährleistet werden. Um diese Ziele zu erreichen, darf jedoch der technische Fortschritt nicht eingeschränkt werden. Daher wird die Wahl der technischen Lösung im Gesetzesentwurf nur geregelt, wenn dies für die Erreichung der gesetzgeberischen Ziele absolut erforderlich ist. Die Vorlage sieht insbesondere eine dezentrale Datenverwaltung vor und schliesst somit jede technische Lösung aus, bei der eine Anbieterin von Identifizierungsdienstleistungen zwischen die Inhaberin oder den Inhaber und die Verifikatorin eines elektronischen Nachweises geschaltet wird. Die Inhaberinnen und Inhaber haben auf diese Weise eine grössere Kontrolle über ihre Daten. Die Mehrheit der Fragen im Zusammenhang mit der Wahl der Technologie ist jedoch nicht auf Gesetzesstufe geregelt. Angesichts der raschen technischen Fortschritte sollte sichergestellt werden, dass dieser Gesetzesentwurf nach dem Inkrafttreten in demjenigen technologischen Kontext umgesetzt werden kann, der dann vorliegt und heute noch nicht bekannt ist.

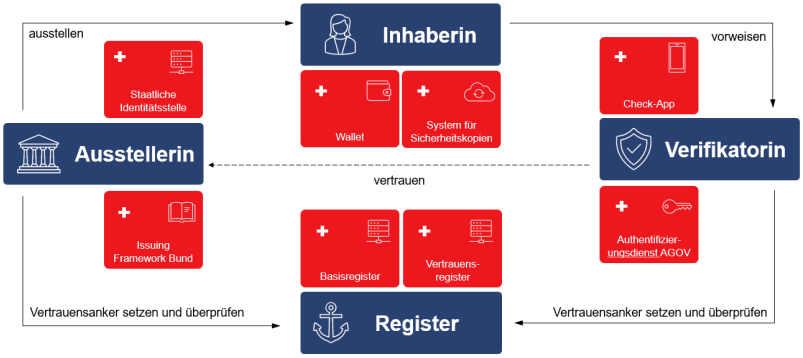
Verschiedene Aspekte, die auf Verordnungsebene geregelt werden müssen, werden technologisch viel konkreter und spezifischer sein. Die Verordnung muss die Interoperabilität aller die Kommunikation betreffenden Systeme gewährleisten. Dazu muss sie namentlich die Datenformate und die Schnittstellen sehr genau festlegen. Dabei sollte der Grundsatz beachtet werden, dass nur absolut notwendige technologische Entscheide getroffen werden sollten. Soweit wie möglich sollte es den verschiedenen Akteuren überlassen werden, die Technologie zu wählen, die sie für die

Formatierung, Speicherung und Bearbeitung der Daten auf ihrer Seite der Schnittstelle verwenden wollen.

2. Abschnitt Vertrauensinfrastruktur

Mit dem Gesetzesentwurf hat der Bund die Kompetenz, eine Informatikinfrastruktur einzuführen, zu entwickeln und zu betreiben, mit der elektronische Nachweise ausgestellt, verwendet, verwaltet, bestätigt und widerrufen werden können. Die Vertrauensinfrastruktur setzt eine Reihe von Normen und Standards, Prozessen, Konzepten und Infrastrukturelementen um, die die Konformität und das Vertrauen des Systems gemäss bewährten Verfahren gewährleisten. Mit der Vertrauensinfrastruktur sollen die Ausstellung, der Widerruf und die Verwendung der E-ID und anderer elektronischer Nachweise ermöglicht werden.

Es gibt drei Arten von Akteuren innerhalb der Vertrauensinfrastruktur: die Ausstellerinnen, die Inhaberinnen und Inhaber und die Verifikatorinnen. Ihre Interaktionen basieren auf festgelegten Kommunikationsstandards. Die vom Bund eingeführte Vertrauensinfrastruktur setzt sich aus folgenden Elementen zusammen: dem Basisregister (Art. 2), dem Vertrauensregister (Art. 3), der Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen (Art. 7) und der Anwendung zur Prüfung von elektronischen Nachweisen (Art. 8). Das Informationssystem (Art. 25) und der Authentifizierungsdienst der Bundeskanzlei (Änderung anderer Erlasse, Bundesgesetz vom 17. März 2023 über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben [EMBAG][21]) mit der E-ID ergänzen die zentralen Elemente dieser Vorlage.



21 BBl **2022** 805

Das BIT stellt die verschiedenen Elemente der Vertrauensinfrastruktur zur Verfügung und betreibt sie. Für die Haftung für Schäden, die bei der Verwendung der E-ID oder der Vertrauensinfrastruktur verursacht werden können, gelten die üblichen Haftungsregeln des Obligationenrechts[22] oder des Verantwortlichkeitsgesetzes vom 14. März 1958[23] (VG).

Art. 2 Basisregister

Abs. 1

Das BIT stellt interessierten Behörden und Privaten ein Basisregister zur Verfügung. Dieses Register stellt einen zentralen Bestandteil der Vertrauensinfrastruktur dar und bildet den ersten Teil des Vertrauensankers des Systems. Mit dem Basisregister kann sich eine Verifikatorin vergewissern, dass die elektronischen Nachweise nicht nachträglich geändert wurden und von den im Basisregister eingetragenen Ausstellerinnen und den zugehörigen Identifikatoren stammen.

Das Basisregister kann in verschiedenen Formen bereitgestellt werden. Die Wahl der technischen Lösung ist jedoch im Gesetzesentwurf nicht geregelt, der soweit möglich technologieneutral sein soll (vgl. Erläuterungen zu Art. 1 Abs. 2 Bst. d). Deshalb sind die technischen Bestandteile des Basisregisters im Gesetzesentwurf nicht detailliert geregelt; dieser sieht lediglich die Funktionen vor, die das Basisregister erfüllen muss. Das Basisregister kann beispielsweise folgende Daten enthalten: die Identifikatoren der Ausstellerinnen und Verifikatorinnen; die kryptografischen Schlüssel, die erforderlich sind, um deren Identifikatoren zu kontrollieren und um die Authentizität und Integrität der elektronischen Nachweise zu überprüfen; die Daten über den Widerruf elektronischer Nachweise. Die Adressen, Telefonnummern, E-Mail-Adressen oder sonstige Kontaktangaben der Ausstellerinnen und Verifikatorinnen sowie die Personendaten der Inhaberinnen und Inhaber werden im Basisregister nicht erfasst.

Abs. 2

Die Ausstellerinnen können ihre Daten selber in das Basisregister eintragen. Dies ermöglicht den Verifikatorinnen, die Integrität und (nur in Bezug auf die von den Ausstellerinnen eingetragenen Daten) die Authentizität der von der jeweiligen Ausstellerin ausgestellten elektronischen Nachweise zu überprüfen. Diese Daten werden beim Eintragen durch einen kryptografischen Algorithmus gesichert und gelten als fälschungssicher.

Ausstellerinnen und Verifikatorinnen, die sich im Vertrauensregister nach Artikel 3 anmelden möchten, müssen ihre Informationen im Basisregister eintragen. Dabei wird die Identität der Ausstellerinnen oder Verifikatorinnen nicht überprüft. Mit einer Eintragung im Basisregister kann lediglich kontrolliert werden, ob gewisse Informationen, wie ein öffentlicher Schlüssel, zu einem bestimmten Identifikator gehören, aber es handelt sich nicht um eine überprüfte Identität. Die Zugehörigkeit eines Identifikators zu einem Akteur kann mit dem Vertrauensregister bestätigt werden (vgl. Erläuterungen zu Art. 3).

22 SR **220**
23 SR **170.32**

Abs. 3

Mit Ausnahme der Daten zum Widerruf enthält das Basisregister keine Daten über die elektronischen Nachweise, wie persönliche Daten oder Angaben zur Ausstellung der elektronischen Nachweise.

Abs. 4

Die Daten zum Widerruf elektronischer Nachweise lassen weder Rückschlüsse auf die Identität der Inhaberin oder des Inhabers noch auf den Inhalt des elektronischen Nachweises zu.

Abs. 5

Die Vernehmlassung hat ergeben, dass die Anforderungen an die Verwendung der Personendaten, die bei Abfragen des Basisregisters anfallen, genauer geregelt werden sollten. Zu diesen Daten gehören namentlich die IP-Adressen und andere ähnliche Daten gemäss dem benutzten Protokoll. Dieser Absatz orientiert sich, sowohl für die Aufzeichnung der Daten als auch für deren (nicht personenbezogene) Auswertung, an den Zwecken, wie sie in Artikel 57*l* Buchstabe b Ziffern 1-3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[24] (RVOG) aufgeführt sind. Absatz 5 hält zudem fest, dass diese Daten nach Artikel 57*n* Buchstabe a RVOG auch personenbezogen, aber nicht namentlich, resp. personenbezogen und namentlich nach Artikel 57*o* Absatz 1 Buchstabe a und b RVOG ausgewertet werden dürfen.

Dazu ist anzumerken, dass das BIT keinen Zugriff hat auf den Inhalt der Transaktionen zwischen den Ausstellerinnen, Inhaberinnen und Inhabern und Verifikatorinnen.

Art. 3 Vertrauensregister

Abs. 1

Das BIT stellt ein öffentlich zugängliches System (Vertrauensregister) zur Verfügung, das Daten für die Verifizierung der Identität von Ausstellerinnen und Verifikatorinnen und für die sichere Verwendung elektronischer Nachweise enthält. Dieses System bildet den zweiten Teil des Vertrauensankers des Systems: Es ermöglicht den Inhaberinnen und Inhabern elektronischer Nachweise und den Verifikatorinnen in Erfahrung zu bringen, mit wem sie es effektiv zu tun haben. Neben der Überprüfung der Identifikatoren stellt das System den Nutzerinnen und Nutzern auch eine Vielzahl von weiteren Informationen zur Verfügung. So kann beispielsweise überprüft werden, ob eine Ausstellerin berechtigt ist, eine bestimmte Art von elektronischem Nachweis auszustellen (fedpol ist z. B. die einzige Ausstellerin der E-ID) oder ob eine Verifikatorin einen besonderen elektronischen Nachweis oder gewisse Informationen, die darin enthalten sind, verlangen darf (z. B. ob ein Akteur die AHV-Nummer der E-ID verlangen darf).

Jeder Akteur kann frei entscheiden, wann er das Vertrauensregister aufruft. Für die kryptografische Überprüfung elektronischer Nachweise oder die Erstellung von sicheren Kommunikationskanälen ist das Vertrauensregister nicht erforderlich. Es kann jedoch das Vertrauen, das ein Akteur bei seinem Gegenüber geniesst, stärken, wenn

24 SR **172.010**

zwischen den beiden keine Beziehung besteht, wenn einer von beiden mehr Informationen wünscht oder wenn eine Bestätigung der Authentizität und der Richtigkeit der geteilten Informationen erforderlich ist.

Das Vertrauensregister ist so gestaltet, dass es sowohl automatische als auch manuelle Anfragen beantworten kann. Diese Informationen werden hauptsächlich von den Anwendungen für die Aufbewahrung und Vorweisung (elektronische Brieftaschen) und den von den Verifikatorinnen verwendeten Systemen genutzt, um die Nutzerinnen und Nutzer besser zu leiten und ihnen zu ermöglichen, fundierte Entscheide zu treffen.

Um den Datenfluss zu minimieren und die dezentrale Art der Vertrauensinfrastruktur beizubehalten, kann jede Bestätigung des Systems als elektronischer Nachweis oder als ähnlicher Ausweis nach dem Stand der Technik ausgestellt werden. Diese elektronischen Nachweise können von einer Ausstellerin oder einer Verifikatorin jedem interessierten Akteur vorgewiesen werden, der dafür nicht das Vertrauensregister aufzurufen braucht. Dabei handelt es sich um eine Anwendungsoption des Vertrauensregisters, die sich in der Evaluationsphase befindet.

Abs. 2

Das BIT ist für die Richtigkeit der öffentlich zugänglichen Informationen im Vertrauensregister verantwortlich. Es hat den Auftrag, die erforderlichen Prozesse einzuführen, um die Qualität und Richtigkeit der Informationen sicherzustellen und diese gegebenenfalls zu berichtigen oder zu aktualisieren.

Abs. 3

Zur Stärkung des Vertrauens in die E-Government-Dienste, die die Vertrauensinfrastruktur einsetzen, werden die Bundes-, Kantons- oder Gemeindebehörden auf ihr Gesuch hin im Vertrauensregister eingetragen. Der Eintrag bestätigt, dass der im Basisregister eingetragene Identifikator zu ihnen gehört.

Abs. 4

Der Bundesrat kann vorsehen, dass der Bund auch den Identifikator von privaten Ausstellerinnen und Verifikatorinnen bestätigt. Mit einer solchen Massnahme kann das Vertrauen, das die Vertrauensinfrastruktur im Bereich der elektronischen Identifizierung geniesst, gestärkt werden. Auch wenn die privaten Ausstellerinnen und Verifikatorinnen grundsätzlich an der Nutzung des Vertrauensregisters interessiert sind, ist es nicht sicher, dass sie dieses auch tatsächlich nutzen werden, wenn es einmal zur Verfügung steht. Ob sich diese Absichten konkretisieren, wird erst nach dem Inkrafttreten dieses Gesetzesentwurfs festgestellt werden können.

In diesem Fall sollten die Anforderungen für die Bestätigung des Identifikators dieser Akteure in einer Verordnung festgelegt werden. Weiter sind auch die technischen und organisatorischen Massnahmen vorzusehen, die zur Gewährleistung der Qualität der im Vertrauensregister bereitgestellten Informationen ergriffen werden müssen.

Schliesslich ist es möglich, dass die privaten Akteure entscheiden, selber und separat nicht staatliche (private) Vertrauensregister bereitzustellen; dieser Gesetzesentwurf schränkt ihre Aktivitäten in diesem Bereich nicht ein.

Abs. 5

Mit diesem Absatz soll den Nutzerinnen und Nutzer ermöglicht werden, im Vertrauensregister zu prüfen, ob der Identifikator einer Ausstellerin oder Verifikatorin vom BIT bestätigt wurde. Die Bestätigungen der Identifikatoren nach den Absätzen 3 und 4 müssen im Vertrauensregister eingetragen sein.

Abs. 6

Die Vernehmlassung hat ergeben, dass die Anforderungen an die Verwendung der Personendaten, die bei Abfragen des Vertrauensregisters anfallen, genauer geregelt werden sollten. Die Bestimmungen lauten gleich wie in Artikel 2 Absatz 5; Absatz 6 verweist daher auf diese, um Wiederholungen zu vermeiden und die Lektüre zu erleichtern (vgl. Erläuterungen zu Art. 2 Abs. 5).

Zusammenfassend ergibt sich, dass die Personendaten, die bei Abfragen des Vertrauensregisters anfallen, nach den Zwecken von Artikel 57*l* Buchstabe b Ziffern 1–3 RVOG aufgezeichnet und nicht personenbezogen ausgewertet werden dürfen, nach den Zwecken von Artikel 57*n* Buchstabe a RVOG auch personenbezogen, aber nicht namentlich resp. nach den Zwecken von Artikel 57*o* Absatz 1 Buchstabe a und b RVOG personenbezogen und namentlich ausgewertet werden dürfen.

Abs. 7

Dieser Absatz überträgt dem Bundesrat die Kompetenz, Regeln für die Bereitstellung anderer Informationen vorzusehen, die eine sichere Nutzung der elektronischen Nachweise gewährleisten. Dabei kann es sich insbesondere um Daten handeln, wie elektronische Nachweise verwendet werden, oder um Daten, anhand derer festgestellt werden kann, ob eine Ausstellerin oder Verifikatorin eine bestimmte Art von elektronischem Nachweis ausstellen und überprüfen soll. Mit dieser Kompetenzdelegation kann zudem das Vertrauensregister weiterentwickelt und besser an die Bedürfnisse des Ökosystems und die technische Entwicklung angepasst werden.

Art. 4 Ausstellung

Abs. 1

Alle Behörden und Private können die Vertrauensinfrastruktur des Bundes nutzen, um elektronische Nachweise auszustellen (andere als die staatliche E-ID, die nur von fedpol ausgestellt wird). Es handelt sich um eine Kann-Bestimmung, so dass Behörden und Private nicht zu deren Nutzung verpflichtet sind. Die Arten elektronischer Nachweise, die ausgestellt werden können, werden zudem in diesem Absatz nicht beschränkt; die Vertrauensinfrastruktur soll verschiedenen Akteuren zur Verfügung stehen und ihnen ermöglichen, elektronische Nachweise unterschiedlichster Art auszustellen.

Diese Bestimmung ist absichtlich offen formuliert, um weder den Kreis der Ausstellerinnen noch die Art der elektronischen Nachweise von vornherein einzuschränken. Aus dem gleichen Grund wurde darauf verzichtet, Vorschriften betreffend die Informationen vorzusehen, die die Ausstellerinnen zu den von ihnen bereitgestellten Nachweisen aufbewahren müssen. Diese Entscheide müssen im Einzelfall von den

Ausstellerinnen selber getroffen werden oder, bei öffentlichen Ausstellerinnen, durch den zuständigen Gesetzgeber.

Für das BIT, das für die Einführung der verschiedenen Komponenten der Vertrauensinfrastruktur nach den Artikeln 2 und 3 zuständig ist, stellt dieser Absatz keine Kann-Bestimmung dar.

Abs. 2

Die elektronischen Nachweise enthalten unterschiedliche Daten. Neben dem von der Ausstellerin festgelegten Basisinhalt gehören dazu solche, die für die Überprüfung der Authentizität und der Integrität erforderlich sind, Dabei kann es sich namentlich um eine elektronische Signatur handeln.

Art. 5 Widerruf

Gemäss dem Gesetzesentwurf haben die Ausstellerinnen das Recht, elektronische Nachweise via Basisregister zu widerrufen; sie sind aber nicht dazu verpflichtet. Sie können selber entscheiden, wann die Nachweise widerrufen werden und das mit der Inhaberin oder dem Inhaber vertraglich festlegen. Dritte, also Behörden oder Private, sind im Übrigen nicht befugt, die von anderen Akteuren ausgestellten elektronischen Nachweise zu widerrufen.

Dieser Artikel legt keine Mindestanforderungen an den Widerruf fest, da die Arten und die Fälle der Nutzung elektronischer Nachweise sehr unterschiedlich sind und verschiedenen Gesetzen unterstehen. Mit diesem Artikel soll lediglich verdeutlicht werden, dass die elektronischen Nachweise von den Ausstellerinnen widerrufen werden können. Ein widerrufener elektronischer Nachweis kann nicht mehr aktiviert werden: Die Ausstellerin kann aber jederzeit einen neuen elektronischen Nachweis ausstellen, mit gleichem oder mit anderem Inhalt. Die Ausstellerinnen können entscheiden, nicht widerrufbare elektronische Nachweise auszustellen, wenn ein Widerruf nicht sinnvoll oder vorgeschrieben ist, und wenn das Verfahren zur Prüfung der Identität zu aufwändig und kompliziert wäre.

Obwohl der Gesetzentwurf keine Widerrufspflicht vorsieht, sind die Ausstellerinnen nach Artikel 6 Absatz 5 DSG gehalten, alle geeigneten Massnahmen zu treffen, um Daten, welche gemessen an den Zwecken, für die sie erhoben oder bearbeitet wurden, unrichtig oder unvollständig sind, zu berichtigen oder zu löschen. Die Ausstellerinnen müssen somit andere technische Massnahmen vorsehen, um die Anforderungen dieser Bestimmung umzusetzen.

Art. 6 Form und Aufbewahrung von elektronischen Nachweisen

Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket. Dieses Datenpaket ist auf einem technischen Träger gespeichert, den die Inhaberin oder der Inhaber wählen kann. Der Gesetzesentwurf enthält keine Anforderungen an die technischen Mittel, die zur Aufbewahrung des elektronischen Nachweises verwendet werden müssen. Der Bund stellt aber eine solche Anwendung zur Verfügung, die strikt nach den Grundsätzen Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen konzipiert ist (vgl. Erläuterungen zu Art. 7).

Art. 7 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Abs. 1

Das BIT stellt eine Anwendung zur Aufbewahrung und Vorweisung der elektronischen Nachweise, eine sogenannte staatliche elektronische Brieftasche, zur Verfügung. Es handelt sich um eine Software-Anwendung, mit der elektronische Nachweise in einer für die Nutzerinnen und Nutzer transparenten und nachvollziehbaren Weise beantragt, sicher bezogen, aufbewahrt, ausgewählt, kombiniert und geteilt werden können. Darin können die E-ID sowie andere elektronische Nachweise verwaltet werden. Soweit dies erforderlich ist, wird bei der Bereitstellung der staatlichen elektronischen Brieftasche den von der EU erarbeiteten Standards Rechnung getragen.

Die Verwendung elektronischer Brieftaschen, die von anderen Akteuren ausgestellt werden, ist im Gesetz nicht geregelt. Neben der staatlichen elektronischen Brieftasche können die Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden.

Abs. 2

Nach dem Verlust eines Smartphones oder dem Kauf eines neuen Smartphones hat es sich bei den Nutzerinnen und Nutzer eingebürgert, die installierten Anwendungen aus einem Backup wiederherzustellen. So können die Funktionalitäten des alten Systems bei einem Wechsel des Smartphones rasch wieder verfügbar gemacht werden. Die gleiche Möglichkeit kann den Inhaberinnen und Inhabern der staatlichen elektronischen Brieftasche angeboten werden.

Als Basisfunktion dieser Anwendung ist vorgesehen, dass auf einem lokalen Datenträger der Inhaberin oder des Inhabers eine Sicherungskopie der elektronischen Nachweise erstellt werden kann.

Dieser Absatz gibt dem Bundesrat die Kompetenz, vorzusehen, dass das BIT ein Informatiksystem bereitstellt, in dem die Inhaberinnen und Inhaber Kopien ihrer elektronischen Nachweise speichern können. Nach einem Wechsel des technischen Trägers (Smartphone, Computer usw.) können sie die gespeicherten elektronischen Nachweise rasch wiederherstellen.

Die Nutzung des Systems für Sicherheitskopien ist freiwillig und nur für Nutzerinnen und Nutzer der Anwendung nach diesem Artikel möglich. Allen Inhaberinnen und Inhabern steht es frei, die Möglichkeit zur Sicherung der elektronischen Nachweise zu nutzen.

Nur die Inhaberinnen und Inhaber können auf ihre Sicherheitskopien zugreifen. Das BIT hat das System so auszugestalten, dass Dritte nicht darauf zugreifen können.

Abs. 3

Dieser Absatz überträgt dem Bundesrat die Kompetenz, Fälle von längerer Inaktivität im Aufbewahrungssystem zu regeln, insbesondere wenn die Sicherheitskopien nicht

aktualisiert oder von den Inhaberinnen und Inhabern über längere Zeit nicht verwendet werden. Mit dieser Massnahme ist es möglich, Daten zu vernichten, um das im Zeitverlauf akkumulierte Datenvolumen zu reduzieren. Mit einer Umsetzung, die den Anforderungen des Datenschutzes und der Datenminimierung entspricht, wird es nicht möglich sein, die Inhaberin oder den Inhaber zu kennen und sie oder ihn vor einer allfälligen Vernichtung der Daten zu kontaktieren. Fristen von zwei bis fünf Jahren werden in einer Verordnung vorgesehen.

Art. 8 Anwendung zur Prüfung von elektronischen Nachweisen

Abs. 1

Das BIT stellt eine Anwendung zur Verfügung, mit der die E-ID auf ihre Gültigkeit überprüft werden kann. Mit dieser Sicherheitsmassnahme soll eine sichere Prüfung der E-ID gewährleistet und erleichtert werden. Zudem kann damit das Vertrauen, das die gesetzlich vorgesehene Infrastruktur geniesst, gestärkt werden. Die Nutzung der Anwendung ist freiwillig: Es steht allen Verifikatorinnen frei, die Anwendung zur Überprüfung der von fedpol ausgestellten E-ID einzusetzen.

Abs. 2

Der Bundesrat kann beschliessen, dass mit dieser Anwendung auch andere elektronische Nachweise auf ihre Gültigkeit überprüft werden können. Diese Möglichkeit könnte eine wichtige Massnahme sein, um die Benutzung der Vertrauensinfrastruktur und der elektronischen Nachweise zu erleichtern. Die Nutzung der Anwendung zur Prüfung der Gültigkeit anderer elektronischer Nachweise wird ebenfalls freiwillig sein. Alle Verifikatorinnen können frei entscheiden, ob sie die Anwendung des Bundes oder eine andere auf dem Markt verfügbare, gleichwertige Anwendung nutzen wollen.

Art. 9 Vorweisen von elektronischen Nachweisen

Abs. 1

Inhaberinnen und Inhaber sind nicht verpflichtet, die elektronischen Nachweise vollumfänglich vorzuweisen. Sie können frei entscheiden, welche Bestandteile des Nachweises oder davon abgeleitete Aussagen sie der Verifikatorin vorweisen, um das Ziel der erforderlichen Überprüfung in einem konkreten Fall zu erreichen. Die konkrete Ausgestaltung der elektronischen Nachweise wird auf dem Verordnungsweg definiert werden, damit gewährleistet ist, dass die Ausstellerinnen die Möglichkeit der Übertragung bestimmter oder sämtlicher Elemente eines elektronischen Nachweises vorsehen.

Der Gesetzesentwurf enthält keine Anforderungen an die Art der Daten, die bei der Überprüfung der elektronischen Nachweise übermittelt werden müssen. Zudem muss die technische Umsetzung ermöglichen, die Bestandteile eines elektronischen Nachweises einzeln vorzuweisen, während die Überprüfung der Authentizität und der Integrität vollumfänglich möglich bleibt.

Die Verifikatorin legt fest, welche Daten im jeweiligen Fall erforderlich sind. Der Handlungsspielraum der Inhaberin oder des Inhabers wird somit durch die Anforderungen begrenzt, die die Verifikatorinnen für den Überprüfungsprozess festlegen. Beschliesst eine Inhaberin oder ein Inhaber, die erforderlichen Elemente nicht zu übermitteln, kann sie oder er möglicherweise nicht auf den Dienst der Verifikatorin zugreifen.

Das DSG setzt jedoch Grenzen dafür, was die Verifikatorinnen von einer Inhaberin oder einem Inhaber eines elektronischen Nachweises verlangen dürfen. So hält Artikel 6 Absatz 2 DSG fest, dass die Bearbeitung von Personendaten nach Treu und Glauben erfolgen und verhältnismässig sein muss. Ausserdem dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden, und sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist (Art. 6 Abs. 3 DSG).

Abs. 2

Das BIT gestaltet die Vertrauensinfrastruktur in der Weise, dass die Ausstellerin eines elektronischen Nachweises keine Kenntnis der Informationen im Zusammenhang mit dessen Vorweisung und Überprüfung hat.

Abs. 3

Das Basisregister und das Vertrauensregister ermöglichen dem BIT nicht, auf den Inhalt der vorgewiesenen elektronischen Nachweise zuzugreifen, weil diese Daten nicht in diesen Registern gespeichert werden. Zudem kann es keine Rückschlüsse auf die Verwendung eines elektronischen Nachweises und die betroffenen Behörden und Privaten ziehen. Als Betreiber der Vertrauensinfrastruktur hat es jedoch Zugriff auf die Personendaten, die bei Abfragen des Basisregisters nach Artikel 2 und des Vertrauensregisters nach Artikel 3 anfallen, beispielsweise auf die IP-Adressen oder andere ähnliche Informationen gemäss benutztem Protokoll.

Art. 10 Meldepflicht der Ausstellerinnen und Verifikatorinnen

Die Vernehmlassung hat auch ergeben, dass eine Meldepflicht für Cyberangriffe auf die Ausstellungs- und Verifikationssysteme vorgesehen werden sollte. Da das BIT nicht über die erforderlichen Zugriffsrechte verfügt, ist es nicht in der Lage, solche Angriffe auf die mit der Vertrauensinfrastruktur verbundenen Systeme wahrzunehmen. Diese Meldepflicht ist daher wichtig, um einen wirksamen Schutz der Nutzerinnen und Nutzer der Vertrauensinfrastruktur des Bundes sicherzustellen.

Die Bestimmung sollte allerdings mit der geplanten Änderung des Informationssicherheitsgesetzes vom 18. Dezember 2020[25] (ISG) abgestimmt werden, die das Parlament derzeit berät.[26] Artikel 74*b* sieht eine neue Meldepflicht bei Cyberangriffen

25 SR 128
26 Botschaft vom 2. Dezember 2022 zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), BBl 2023 84; www.parlament.ch > Ratsbetrieb > Suche Curia Vista > 22.073

auf kritische Infrastrukturen vor. Für den Fall, dass das Parlament die Gesetzesänderung verabschiedet und diese in Kraft tritt, sieht der Entwurf folgende koordinierende Bestimmung vor:

Art. 74b Bst. v

[1] Die Meldepflicht gilt für:

> v. Ausstellerinnen und Verifikatorinnen von elektronischen Nachweisen im Sinn des Bundesgesetzes vom … über den elektronischen Identitätsnachweis und andere elektronische Nachweise.

Art. 11 Quellcode der Vertrauensinfrastruktur

Abs. 1

Der Bund veröffentlicht den Quellcode der Bestandteile der Vertrauensinfrastruktur nach den Buchstaben a–d im Internet. Mit dieser Massnahme soll das Vertrauen, das die Vertrauensinfrastruktur bei der Bevölkerung geniesst, gestärkt und ein hohes Sicherheitsniveau aufrechterhalten werden, indem Interessierten ermöglicht wird, den offen gelegten Code zu testen. Dieser Absatz hat zudem zum Ziel, die Offenheit beizubehalten, die Teil des partizipativen Ansatzes der Vorlage ist.

Abs. 2

Das BIT kann ausnahmsweise entscheiden, den Quellcode oder Teile davon nicht zu veröffentlichen, wenn Grund zur Annahme besteht, dass die IT-Sicherheit eines der in Absatz 1 Buchstaben a-d aufgeführten Elemente durch die Publikation gefährdet würde. So wäre beispielsweise denkbar, den Quellcode von Elementen, die den Online-Prozess der Identitätsprüfung betreffen, nicht zu veröffentlichen, soweit dieser Prozess mittels der in Artikel 7 genannten Anwendung (staatliche elektronische Brieftasche) abgewickelt wird.

Der Gesetzesentwurf sieht keine ausdrückliche Regelung über die technischen und organisatorischen Massnahmen vor, die im Bereich der Vertrauensinfrastruktur zu ergreifen sind. Um Wiederholungen zu vermeiden und das Verständnis zu erleichtern, verweist der Gesetzesentwurf hier nicht auf Artikel 8 DSG, Artikel 3 und 4 der Verordnung vom 31. August 2022 zum Datenschutzgesetz[27] (VDSG) und auf die Bestimmungen des ISG; das BIT wird geeignete technische und organisatorische Massnahmen vorsehen, damit beim Betrieb der Vertrauensinfrastruktur eine hohe und den Risiken entsprechende Datensicherheit gewährleistet ist. Der Entwurf sieht auch keine ausdrückliche Verpflichtung des BIT vor, regelmässige, in diesem Bereich national und international anerkannte Kontrollen der Schlüsselelemente der Vertrauensinfrastruktur durchzuführen. Es handelt sich hierbei um technische Massnahmen, die in der Praxis typischerweise getroffen werden, um eine hohe Sicherheit der benutzten IT-Infrastruktur sicherzustellen; einer rechtlichen Grundlage bedarf es dafür nicht.

27 SR **235.11**

3. Abschnitt E-ID

Art. 12 Form

Das BIT stellt eine Vertrauensinfrastruktur zur Verfügung (vgl. 1. Abschnitt), die es staatlichen und privaten Akteuren ermöglicht (vgl. Einschränkung in Art. 3 Abs. 4), unterschiedliche Nachweise in elektronischer Form auszustellen, die zum Nachweis der Identität, eines Sachverhalts oder eines Ereignisses verwendet werden können (elektronischer Nachweis). Die E-ID ist ein elektronischer Nachweis, der die Identität der Nutzerin oder des Nutzers belegt und ausschliesslich von fedpol mittels der staatlichen Vertrauensinfrastruktur ausgestellt wird. Namentlich handelt es sich bei der E-ID um ein «beweiskräftiges Dokument» im Sinne von Artikel 3 des Geldwäschereigesetzes vom 10. Oktober 1997[28].

Art. 13 Persönliche Voraussetzungen

Vorbemerkung

Damit eine Person eine E-ID beantragen kann, muss sie bereits über einen von den Schweizer Behörden ausgestellten Ausweis verfügen. Diese Voraussetzung hat den Vorteil, dass so gewährleistet ist, dass diese Person von einer Schweizer Behörde identifiziert wurde und aktuelle Daten von ihr verfügbar sind.

Es besteht keine Verpflichtung, eine E-ID zu beziehen oder zu verwenden. Wenn jedoch die persönlichen Voraussetzungen erfüllt sind, ist fedpol verpflichtet, der antragstellenden Person eine E-ID auszustellen. Durch den Bezug einer E-ID werden die antragstellenden Personen zu Inhaberinnen und Inhabern einer E-ID.

Bst. a

Ziff. 1

Um die Ausstellung einer E-ID zu beantragen, genügt für Schweizer Bürgerinnen und Bürger ein gültiger Ausweis nach dem AwG. Diese Regelung gilt auch für Auslandschweizerinnen und Auslandschweizer. Juristische Personen, die immer durch ihr Organ, also durch natürliche Personen, handeln, können nicht Inhaberinnen und Inhaber einer E-ID sein und werden mittels der einheitlichen Unternehmens-Identifikationsnummer (UID)[29] identifiziert.

Ziff. 2

Alle Ausländerinnen und Ausländer, die eine gültige Bewilligung nach dem AIG und der Verordnung vom 24. Oktober 2007[30] über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE) besitzen, können eine E-ID beziehen. Es handelt sich um folgende Ausweise:

28 SR **955.0**
29 www.bfs.admin.ch > Register > Unternehmensregister > Unternehmens-Identifikationsnummer UID
30 SR **142.201**

- Ausweis L: Kurzaufenthaltsbewilligung (Art. 32 AIG und 71 Abs. 1 VZAE)
- Ausweis B: Aufenthaltsbewilligung (Art. 33 AIG und 71 Abs. 1 VZAE)
- Ausweis C: Niederlassungsbewilligung (Art. 34 AIG und 71 Abs. 1 VZAE)
- Ausweis Ci: Aufenthaltsbewilligung mit Erwerbstätigkeit (Art. 30 Abs. 1 Bst. g, 98 Abs. 2 AIG, Art. 45 und 71*a* Abs. 1 Bst. e VZAE)
- Ausweis N: Ausweis für Asylsuchende (Art. 42 AsylG und Art. 71*a* Abs. 1 Bst. b VZAE)
- Ausweis F: Ausweis für vorläufig aufgenommene Ausländerinnen und Ausländer (Art. 41 Abs. 2 AIG und 71*a* Abs. 1 Bst. c VZAE)
- Ausweis S: Ausweis für Schutzbedürftige (Art. 74 AsylG und 71*a* Abs. 1 Bst. d VZAE)
- Ausweis G: Grenzgängerbewilligung (Art. 35 AIG und Art. 71*a* Abs. 1 Bst. a VZAE)

Es steht ausser Frage, dass mit dieser Regelung nicht alle Ausländerinnen und Ausländer, die in Kontakt mit den Schweizer Behörden sind, berechtigt sind, eine E-ID zu beantragen (z. B. Ausländerinnen und Ausländer, die ein Ferienhaus in der Schweiz besitzen). Da diese Personen nie formell von einer Schweizer Behörde identifiziert wurden, kann ihnen keine E-ID ausgestellt werden. Diese Regelung schliesst nicht aus, dass die Behörden, die in engem Kontakt mit diesen Ausländerinnen und Ausländern stehen, ihnen einen anderen elektronischen Identifizierungsnachweis ausstellen.

Die für Schweizer Bürgerinnen und Bürgern und für Ausländerinnen und Ausländern ausgestellten E-ID sind gleichwertig. Der Bezug einer E-ID bietet jedoch den Inhaberinnen und Inhabern keine Garantie für einen Zugang zu allen damit verbundenen Diensten. Es ist beispielsweise nicht sicher, dass sie damit alle Online-Dienste nutzen können. Gewisse Anbieterinnen können – aus Sicherheitsgründen im Zusammenhang mit der Zuverlässigkeit der Überprüfung der Identität von Ausländerinnen und Ausländern – entscheiden, den Zugang zu ihren Diensten auf Inhaberinnen und Inhaber einer bestimmten Aufenthaltsbewilligung zu beschränken. Der vorliegende Gesetzesentwurf sieht keine Beschränkung des Zugangs zu den Online-Diensten vor und lässt den betreffenden Dienstanbieterinnen diesbezüglich einen Spielraum. Sofern dies gerechtfertigt ist, kann der Zugang zu gewissen Diensten für Inhaberinnen und Inhabern eines Ausländerausweises, deren Identität nicht verlässlich festgestellt werden konnte, eingeschränkt werden.

Für bestimmte Ausweiskategorien (z. B. Ausweise N, F, S und Ci) kann nicht davon ausgegangen werden, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. Viele Asylsuchende können im Asylverfahren keine Identitätsdokumente einreichen, was eine sichere Identifizierung verunmöglicht. Selbst bei vorläufig aufgenommenen Personen werden im EJPD (Staatssekretariat für Migration) zahlreiche Gesuche um Änderung oder Berichtigung von

Personenidentifizierungsdaten eingereicht, wobei diese Gesuche nicht selten mit untauglichen Dokumenten untermauert werden.

Ziff. 3

Alle Ausländerinnen und Ausländer, die eine gültige Legitimationskarte gemäss Artikel 17 Absatz 1 der Gaststaatverordnung vom 7. Dezember 2007[31] (V-GSG) in Verbindung mit Artikel 71*a* Absatz 1 VZAE besitzen, können eine E-ID beziehen.

Bst. b

Dieser Buchstabe sieht vor, dass einer interessierten Person nach Ablauf der Gültigkeitsdauer ihres Ausweises oder ihrer Legitimationskarte eine E-ID ausgestellt werden kann. Die E-ID kann unter zwei Voraussetzungen ausgestellt werden: (1) der Antrag auf Ausstellung eines Ausweises nach dem AwG oder eines Ausweises nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl wurde persönlich eingereicht und (2) der E-ID-Antrag wurde persönlich eingereicht. Die beiden Anträge können der zuständigen Behörde anlässlich des gleichen Termins eingereicht werden. Bevor die zuständige Behörde die E-ID ausstellt, muss sie die Identität der antragstellenden Person prüfen. Die in diesem Absatz vorgesehene Möglichkeit entspricht den Bedürfnissen der Praxis und soll gewährleisten, dass die Ausstellung der E-ID benutzerfreundlich ist.

Art. 14 Inhalt

Abs. 1

Eine E-ID enthält die folgenden Personenidentifizierungsdaten:

a. amtlicher Name;

b. Vornamen;

c. Geburtsdatum;

d. Geschlecht;

e. Heimatort; dabei handelt es sich um eine schweizerische Besonderheit, die in der E-ID beibehalten wird, um gewisse administrative Prozesse in der Schweiz zu erleichtern;

f. Geburtsort; der Geburtsort wird häufig im Rahmen von internationalen Transaktionen verlangt und wurde aus diesem Grund in die E-ID eingefügt;

g. Nationalität; da Ausländerinnen und Ausländer mit einer Schweizer Aufenthaltsbewilligung ebenfalls eine E-ID erhalten können, wird auch die

31 SR **192.121**

Nationalität in der E-ID angegeben; diese Information ist häufig im Rahmen von nationalen und internationalen Transaktionen erforderlich;

h. Gesichtsbild;

i. AHV-Nummer; die AHV-Nummer als eindeutige und lebenslang bestehende Nummer ist sehr nützlich für administrative Abläufe; sie darf nur von den vom Gesetz ermächtigten Behörden aufgerufen werden.

Diese Daten sind in den amtlichen

Registern des Staates verfügbar, auf die fedpol nach Artikel 25 Absatz 3 Zugriff hat; sie werden unverändert in die E-ID übertragen.

Abs. 2

Neben den Personenidentifizierungsdaten enthält eine E-ID zusätzliche Informationen. Es handelt sich um folgende Daten: E-ID-Nummer, Ausstellungs- und Ablaufdatum der E-ID, Angaben zum Ausweis, der bei der Ausstellung verwendet wurde, insbesondere Typ und Gültigkeitsdauer des Ausweises, und Angaben zum Ausstellungsprozess.

Abs 3

Dieser Absatz wurde eingeführt, um den Ergebnissen des Vernehmlassungsverfahrens Rechnung zu tragen. Verschiedene Vernehmlassungsteilnehmende haben betont, dass die Ausweise der E-ID-Inhaberinnen und Inhaber auch zusätzliche Daten enthalten können, wie z. B. den Namen der gesetzlichen Vertreterin oder des gesetzlichen Vertreters, den Allianz-, Ordens- Künstler- oder Partnerschaftsnamen und die Angabe von besonderen Kennzeichen. Solche Angaben können in gewissen Fällen für Transaktionen der Inhaberinnen und Inhaber der E-ID nützlich oder sogar erforderlich sein. Sie können in der E-ID enthalten sein, wenn sie auch im Ausweis, in einem anderen Ausweispapier oder in der Legitimationskarte der Inhaberin oder des Inhabers angegeben sind.

Art. 15 Antrag

Abs. 1

Es besteht keine Pflicht, eine E-ID zu beziehen. Wenn eine Person eine E-ID erhalten will, muss sie diese bei fedpol beantragen. Der Antrag muss von der späteren Inhaberin oder dem späteren Inhaber der E-ID (antragstellende Person) ausgehen und gegebenenfalls von ihrer bzw. seiner gesetzlichen Vertretung genehmigt werden (s. Abs. 3 für Minderjährige und Personen unter umfassender Beistandschaft). Die antragstellende Person oder ihre gesetzliche Vertretung kann die Ausstellung einer E-ID direkt über das Informationssystem von fedpol oder über die staatliche elektronische Brieftasche (Art. 7) beantragen.

Abs. 2

Um den Vernehmlassungsergebnissen Rechnung zu tragen, sieht Absatz 2 die Möglichkeit vor, gleichzeitig mehrere E-ID zu beziehen. Die Vernehmlassung hat ergeben, dass in der Praxis ein solches Bedürfnis besteht. Ein Elternteil kann beispielsweise die E-ID seines Kindes benötigen, um Transaktionen in dessen Namen durchzuführen. Für gewisse Personen könnte es nützlich sein, ihre E-ID auf mehreren technischen Trägern zu speichern, beispielsweise auf einem privaten Smartphone, einem beruflichen Smartphone, einem Tablet oder einem Laptop. Um allfällige Missbräuche zu verhindern, wird jedoch vorgesehen, dass die Ausstellung gleichzeitig erfolgen muss. Sobald eine oder mehrere E-ID ausgestellt sind, kann die Inhaberin oder der Inhaber nicht die Ausstellung einer zusätzlichen E-ID auf einem anderen Träger beantragen (ohne dass die bereits bestehenden E-ID vorher widerrufen wurden [Art. 18 Bst. e]). In diesem Fall muss sie oder er einen neuen Antrag für alle Träger einreichen, und die alten E-ID werden widerrufen.

Abs. 3

Nach diesem Absatz benötigen Minderjährige und Personen unter umfassender Beistandschaft für den Bezug einer E-ID die Einwilligung ihrer gesetzlichen Vertretung. Das Erfordernis orientiert sich an der Altersgrenze, die für den Bezug eines schweizerischen Ausweises gilt (18 Jahre; Art. 5 Abs. 1 AwG). Die gesetzliche Vertretung von Minderjährigen und von Personen unter umfassender Beistandschaft kann deren E-ID und die eigene E-ID in der elektronischen Brieftasche nach Artikel 7 aufbewahren.

Art. 16 Identitätsprüfung

Abs. 1

Dieser Absatz wurde eingeführt, um den Vernehmlassungsergebnissen Rechnung zu tragen. Viele Vernehmlassungsteilnehmende waren der Ansicht, dass der Gesetzesentwurf die Möglichkeit vorsehen sollte, die E-ID persönlich vor Ort zu beziehen. So ermöglicht die Bestimmung der antragstellenden Person, ihre Identität online bei fedpol oder persönlich bei den von den Kantonen bezeichneten zuständigen Stellen oder Behörden in der Schweiz oder den vom Bundesrat bezeichneten Stellen oder Behörden im Ausland prüfen zu lassen. Mit den Kantonen wurden Konsultationen in die Wege geleitet, um abzuklären, ob Verfahren zur Überprüfung der Identität u.a. auch in Passbüros oder kantonalen Migrationsämtern eingeführt werden könnten.

Abs. 2

Dieser Absatz ermächtigt die in Absatz 1 genannten Behörden und Stellen, durch einen Abgleich zu überprüfen, ob das Gesicht der antragstellenden Person dem in den Registern des Bundes (ISA, ZEMIS oder Ordipro) enthaltenen Gesichtsbild entspricht. Diese Prüfung kann persönlich vor Ort oder online erfolgen. Der Bundesrat wird die Modalitäten des Verfahrens auf Verordnungsstufe regeln (Art. 19 Bst. b).

Abs. 3

Dieser Absatz schafft eine gesetzliche Grundlage im formellen Sinn, die es fedpol erlaubt, biometrische Daten zu sammeln, um den Abgleich nach Absatz 2 durchzuführen. Dieser Abgleich wird während des Online-Prozesses durchgeführt. Absatz 3 setzt somit die Anforderungen von Artikel 34 Absatz 2 Buchstabe a DSG um. Gemäss diesem Artikel ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich, damit Bundesorgane besonders schützenswerte Daten bearbeiten dürfen. Artikel 5 Buchstabe c Ziffer 4 DSG bestimmt, dass «biometrische Daten, die eine natürliche Person eindeutig identifizieren», besonders schützenswerte Daten darstellen. Unter biometrischen Daten sind «Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen»[32].

Im Rahmen der Vernehmlassung forderten einige Teilnehmende, dass die biometrischen Daten, die im Ausstellungsprozess der E-ID anfallen, unverzüglich vernichtet werden. Der Gesetzesentwurf sieht diese Pflicht nicht vor, da fedpol erlaubt werden soll, diese biometrischen Daten aufzubewahren, die zur Untersuchung der Erschleichung einer E-ID erforderlich sind (Art. 26 Abs. 1 Bst. b). Deshalb dürfen diese Daten bis zu fünf Jahren ab dem Ablaufdatum der E-ID aufbewahrt werden.

Art. 17 Ausstellung

Fedpol prüft, ob die antragstellende Person die Voraussetzungen nach Artikel 13 erfüllt. Ist das der Fall, überprüft es ihre Identität mithilfe der erforderlichen Informationen. Dazu vergleicht es die von der antragstellenden Person beigebrachten Informationen mit jenen aus den Registern des Bundes nach Artikel 25 Absatz 3. Wenn die Überprüfung der Identität der antragstellenden Person erfolgreich war, übermittelt ihr fedpol eine E-ID mit den Daten nach Artikel 14.

Die Online-Identitätsprüfung wird in den meisten Fällen automatisiert ablaufen. Bei Unsicherheiten kann fedpol eingreifen und die Daten, die während des Überprüfungsprozesses angefallen sind, überprüfen. Die antragstellende Person hat auch die Möglichkeit, sich beim fedpol zu beschweren. Die Anforderungen von Artikel 21 Absatz 2 DSG müssen im Rahmen dieses automatisierten Prozesses eingehalten werden.

Art. 18 Widerruf

Es muss zwischen Vernichtung und Widerruf der E-ID unterschieden werden.

Die Vernichtung der E-ID ist ein unumkehrbarer Prozess, bei dem das Datenpaket bestehend aus Attributen und kryptografischem Material gelöscht wird. Aus technischer Sicht kann die Ausstellerin eine E-ID aufgrund der dezentralen Art der Vertrauensinfrastruktur nicht vernichten. Nur die Inhaberinnen und Inhaber können ihre E-ID

32 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 6941, hier 7020

löschen, indem sie diese in ihrer elektronischen Brieftasche löschen oder die elektronische Brieftasche auf ihrem Smartphone deinstallieren.

Im Falle eines Widerrufs nimmt fedpol im Basisregister den Eintrag vor, dass eine spezifische E-ID nicht mehr gültig ist. Die entsprechende E-ID bleibt in der elektronischen Brieftasche unverändert und kann weiterhin vorgewiesen werden. Sobald eine Verifikatorin jedoch eine widerrufene E-ID überprüft, sieht sie anhand des Eintrags im Basisregister, dass die betreffende E-ID nicht mehr gültig ist.

Der Gesetzesentwurf sieht die Möglichkeit vor, eine E-ID in den Fällen nach den Buchstaben a–e zu widerrufen. Die Inhaberin oder der Inhaber (erwachsene oder minderjährige Person oder Person unter umfassender Beistandschaft) oder die gesetzliche Vertretung von Minderjährigen oder von Personen unter umfassender Beistandschaft kann den Widerruf der eigenen E-ID oder der E-ID der Person, die sie vertritt, verlangen. Zudem widerruft fedpol die E-ID, wenn der begründete Verdacht besteht, dass sie missbräuchlich verwendet wird. Bevor es eine E-ID widerruft, überprüft es die Informationen hinsichtlich des behaupteten Missbrauchs. Es widerruft die E-ID auch, wenn es informiert wird, dass die Inhaberin oder der Inhaber einer E-ID verstorben ist, oder dass der im Ausstellungsprozess der E-ID verwendete Ausweis entzogen wurde. Diese Informationen gehen bei fedpol in Form von Push-Mitteilungen aus den Registern nach Artikel 25 Absatz 3 ein. Der Bundesrat regelt auf Verordnungsstufe die Pflichten der zuständigen Behörden in Bezug auf den Versand der erforderlichen Mitteilungen.

Ausserdem wird die E-ID widerrufen, wenn eine neue E-ID für dieselbe Person ausgestellt wird. Eine widerrufene E-ID kann nicht mehr aktiviert werden: Die betroffene Person kann jedoch bei fedpol einen neuen Ausstellungsantrag gemäss Artikel 15 Absatz 1 einreichen.

Der Widerruf ist eine technische Massnahme und kann nicht annulliert werden. Zudem kann die Inhaberin oder der Inhaber der E-ID nicht darüber in Kenntnis gesetzt werden, weil der Kanal, der für die Kommunikation mit fedpol verwendet wurde, möglicherweise nicht mehr existiert. Es steht der Inhaberin oder dem Inhaber frei, die E-ID nach Erhalt zu löschen. Der Gesetzesentwurf sieht den Widerruf als technische Massnahme zur Verhinderung von Missbräuchen vor. Es handelt sich um einen Kompromiss zwischen der benutzerfreundlichen Nutzung der E-ID und der Notwendigkeit, ein hohes Sicherheitsniveau zu gewährleisten. Der Widerruf hat nicht den Entzug des Rechts auf eine E-ID zur Folge. Die Inhaberin oder der Inhaber kann einen neuen Ausstellungsantrag einreichen.

Der Widerruf stellt einen Realakt dar und ist deshalb nicht Gegenstand einer Verfügung von fedpol. Die Inhaberin oder der Inhaber kann vom Widerruf Kenntnis nehmen, wenn er die E-ID oder die elektronische Brieftasche benutzt. Sie oder er kann auch den Support von fedpol kontaktieren, um sich zu vergewissern, dass die E-ID widerrufen wurde. Zudem haben sie die Möglichkeit, von fedpol gestützt auf Artikel 25*a* des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[33] (VwVG) den Erlass einer Verfügung zu verlangen. Dafür müssten sie oder er fedpol die notwendigen Daten für den Versand der Verfügung liefern.

33 SR **172.021**

Art. 19 Verfahren

Dieser Artikel delegiert an den Bundesrat die Kompetenz, die Verfahren betreffend Antrag auf Ausstellung einer E-ID (Art. 15), Identitätsprüfung der antragstellenden Person (Art. 16), Ausstellung (Art. 17) sowie Widerruf der E-ID (Art. 18) zu regeln.

Art. 20 Gültigkeitsdauer

Aus Sicherheitsgründen hat die E-ID eine zeitlich befristete Gültigkeit. Der Bundesrat regelt die Anforderungen an diese Dauer in einer Verordnung. In diesem Rahmen sollte geklärt werden, ob die Gültigkeitsdauer der E-ID jener des Dokuments entsprechen muss, das für ihre Ausstellung verwendet wurde. Die Gültigkeitsdauer wird in der E-ID angegeben (Art. 14 Abs. 2 Bst. b und c). Wird der für die Ausstellung der E-ID verwendete Ausweis von den Behörden entzogen, so widerruft fedpol die E-ID, sobald es über den Entzug informiert wird (Art. 18 Bst. d Ziff. 1).

Eine nicht mehr gültige E-ID bleibt auf dem elektronischen Träger der Inhaberin oder des Inhabers als echter, aber abgelaufener elektronischer Nachweis verfügbar.

Art. 21 Sorgfaltspflichten der Inhaberin oder des Inhabers

Abs. 1

Die im Rahmen des Gesetzesentwurfs den Inhaberinnen und Inhabern einer E-ID auferlegten Pflichten entsprechen etwa den Sorgfaltspflichten, die üblicherweise bei der Nutzung von Online-Bankdiensten eingehalten werden müssen. Beispielsweise ist es notwendig und zumutbar, die allenfalls notwendige PIN nicht offenzulegen und nicht mit dem E-ID-Träger zusammen aufzubewahren. Ebenso zumutbar sind beispielsweise die Aktivierung des Zugangsschutzes (z. B. PIN oder Fingerabdruckerkennung) und die Installation eines Virenschutzes auf diesem Gerät. Trotz aller Vorsichtsmassnahmen kann ein Identitätsmissbrauch nie völlig ausgeschlossen werden. Entsprechend können angemessene Strafbestimmungen zur Sanktionierung eines solchen Verhaltens angewendet werden. Bei der Überarbeitung des DSG wurde das Strafgesetzbuch[34] mit einem Artikel 179^{decies} ergänzt, der den Identitätsmissbrauch mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht. Zur Vermeidung von Doppelspurigkeiten enthält der vorliegende Gesetzesentwurf keine Bestimmungen zur Bestrafung desselben Verhaltens.

Abs. 2

Beim Verlust eines physischen Ausweises muss die Polizei umgehend informiert werden (Art. 8 AwG). Eine analoge Regelung für die E-ID macht keinen Sinn. Eine E-ID sollte immer über einen doppelten Schutz verfügen (Sicherung des Zugriffs auf das Gerät und Sicherung des Zugriffs auf die elektronische Brieftasche). Wenn also ein Gerät in die Hände nicht befugter Personen fällt, sollte der Zugriff auf die darauf enthaltene E-ID nicht möglich sein. Die Inhaberin oder Inhaber kann aber jederzeit – also auch im Verlustfall – den Widerruf der E-ID verlangen (Art. 18 Bst. a).

34 SR **311.0**

Wenn die Inhaberin oder der Inhaber den Verdacht hat, dass ihre oder seine E-ID missbräuchlich verwendet wird, muss sie oder er dies unverzüglich an fedpol melden und gegebenenfalls den Widerruf der E-ID verlangen.

Art. 22 Sorgfaltspflicht der Verifikatorinnen

Dieser Artikel wurde dem Gesetz hinzugefügt, um gewissen Forderungen Rechnung zu tragen, die im Rahmen des Vernehmlassungsverfahrens formuliert worden sind. Das Fehlen von Einschränkungen bei der Datenbearbeitung durch die Verifikatorinnen war Gegenstand zahlreicher Kritiken und Vorschläge. Der Hauptkritikpunkt bezieht sich auf den Umstand, dass Verifikatorinnen frei entscheiden können, ob und in welchem Umfang ein elektronischer Nachweis vorgewiesen werden soll. Diese Möglichkeit soll nach Ansicht gewisser Vernehmlassungsteilnehmenden durch Gesetz auf das strikt Notwendige beschränkt und von einer ausdrücklichen Einwilligung abhängig gemacht werden, wozu es einer umfassenden Information über den Zweck der Abfrage bedarf. In gewissen Stellungnahmen wurde auch der Standpunkt vertreten, dass der Gesetzvorentwurf und das DSG die Inhaberinnen und Inhaber elektronischer Nachweise nicht ausreichend vor der Gefahr eines ungerechtfertigten oder unverhältnismässigen Rückgriffs auf die elektronische Identifizierung durch die Verifikatorinnen schützen.

Bei der Erarbeitung dieser Bestimmung wurde zunächst festgestellt, dass wirksame Sanktionen nur im Zusammenhang mit der Verwendung der E-ID verhängt werden können. Die Fälle, in denen andere elektronische Nachweise verwendet werden, sind zu vielfältig und nicht ausreichend bekannt, um einheitliche Sanktionen zu verhängen. Weiter wurde deutlich, dass strafrechtliche Sanktionen nicht das beste Mittel sind, um Verstösse gegen Absatz 1 zu verhindern. Angesichts der strafrechtlichen Sanktionen, die für die Verletzung der verschiedenen Bestimmungen des DSG vorgesehen sind, ist eine Verletzung von Absatz 1 nicht gleich zu gewichten und könnte dadurch nicht durch eine vergleichbare Sanktion geahndet werden. Darüber hinaus lassen die Anforderungen von Absatz 1 einen erheblichen Interpretationsspielraum und eignen sich nicht gut für die Verhängung einer strafrechtlichen Sanktion. Die bewerteten strafrechtlichen Sanktionen würden in der Praxis zu erheblichen Inkonsistenzen und Ungleichheiten führen. Präzisere Anforderungen wie die obligatorische Eintragung in das Vertrauensregister für Verifikatorinnen, die die E-ID verwenden, könnten im Falle einer Missachtung sanktioniert werden, stünden jedoch den Grundprinzipien der SSI diametral entgegen und würden eine erhebliche bürokratische Belastung darstellen. Schliesslich hat sich herausgestellt, dass die Mitteilung von Verstössen an andere Nutzerinnen und Nutzer sowie der Ausschluss der fehlbaren Verifikatorin sinnvollere und wirksamere Sanktionen für das beanstandete Verhalten darstellen.

Die Möglichkeit, andere Aspekte zu regeln, wie eine erweiterte Informationspflicht der Inhaberin resp. des Inhabers, ein erweitertes Widerspruchsrecht der Inhaberin resp. des Inhabers oder ein Kopplungsverbot[35] (Instrumente zur Bekämpfung von

35 I.S.v. Artikel 7 Absatz 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG , ABl. L 119 vom 4.5.2016, S. 1.

«Überidentifikation»), wurde als Reaktion auf die Kritik und die Argumente der Teilnehmerinnen und Teilnehmer der Vernehmlassung geprüft. Angesichts der technischen Schwierigkeiten bei der Umsetzung solcher Anforderungen war es nicht möglich, neue gemeinsame Regeln in diesem Bereich festzulegen. Darüber hinaus möchte der Bundesrat die Diskussion über die vereinbarten Kompromisse bei den Sanktionen im Rahmen des DSG nicht wieder aufnehmen.

Die Bestimmungen des DSG und des Zivilgesetzbuches[36] (ZGB) bleiben hier anwendbar. Die Verarbeitung der in der e-ID enthaltenen Personendaten muss verhältnismässig (angemessen, relevant und nicht übermässig) zu den von der Verifikatorin festgelegten Zwecken sein (Art. 6 Abs. 2 DSG).

Abs. 1

Um die in der Vernehmlassung geäusserten Bedenken aufzunehmen, sollen mit dem Absatz 1 die Anforderungen des DSG und des Vorentwurfs in Bezug auf die Verwendung der E-ID erhöht werden. Er legt die Bedingungen fest, nach denen die Verifikatorinnen die Inhaberinnen und Inhaber auffordern können, in der E-ID enthaltene personenbezogenen Daten zu übermitteln: Nach Absatz 1 können diese Daten nur angefordert werden, wenn die Überprüfung der Identität oder eines Aspekts der Identität der Inhaberin oder des Inhabers gesetzlich vorgeschrieben (Bst. a) oder aus Gründen der Sicherheit der Transaktion erforderlich ist (Bst. b). Absatz 1 soll also Abfragen von Personendaten begrenzen, die für die Erbringung einer Leistung nicht wesentlich sind. Es geht darum, zu verhindern, dass die Verifikatorinnen ungerechtfertigt oder unverhältnismässig elektronische Identifizierung durchführen.

Bst. a

Ein Beispiel für die Übermittlung von Personendaten zu dem in Bst. a genannten Zweck wäre ein Auskunftsgesuch nach Artikel 25 DSG und 16 Absatz 3 DSV. Die Person, die den für die Verarbeitung Verantwortlichen um Zugang zu den relevanten Informationen ersucht, erhält insbesondere Informationen über ihre Identität. Es könnte sich auch um die in Artikel 20 der Verordnung vom 15. November 2017[37] über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) enthaltene Verpflichtung handeln, dass Fernmeldedienstanbieterinnen (FDA) und Wiederverkäufer die Identität der Nutzerin oder des Nutzers überprüfen müssen. Darüber hinaus erfüllt auch Artikel 17 der Geldwäscheverordnung vom 11. November 2015[38] (GwV), der eine Pflicht zur Überprüfung der Identität einer Vertragspartnerin oder des Vertragspartners durch die Händlerin oder der Händler beim Abschluss eines Vertrags vorsieht, die Anforderungen dieses Buchstabens. Darüber hinaus wird die Pflicht zur Identifizierung im Rahmen der Beantragung eines elektronischen Patientendossiers nach der Änderung der Gesetzgebung über das elektronische Patientendossier ebenfalls ein Anwendungsfall dieses Buchstabens sein.

Bst. b

36 SR **210**
37 SR **780.11**
38 SR **955.01**

Bei der Übermittlung personenbezogener Daten für den unter Buchstabe b genannten Zweck könnte es sich um die Überprüfung der Identität einer Person handeln, um eine von einer Universität oder einer anderen Bildungseinrichtung organisierte Prüfung abzulegen. Darüber hinaus könnte es auch notwendig sein, die Identität einer Person bei der Zustellung eines Pakets durch den Lieferdienst zu überprüfen. Die Überprüfung der Identität ist in diesen Fällen ein wesentliches Element.

Die Überprüfung der Identität einer Verbraucherin oder eines Verbrauchers im Rahmen einer Bestellung auf Rechnungen, die sie oder er im Internet tätigt, erfüllt jedoch nicht die Anforderungen von Buchstabe b. Die Verkäuferin oder der Verkäufer könnte sich mit der E-ID vergewissern wollen, dass ihr oder sein Gegenüber volljährig ist und tatsächlich existiert. Dies ist ein echtes und wichtiges Bedürfnis, aber keine Notwendigkeit im Zusammenhang mit der Zuverlässigkeit der Transaktion, die es erforderlich machen würde, dass die Verkäuferin oder der Verkäufer unter anderem die Kreditwürdigkeit oder die Adresse überprüft, um sicherzustellen, dass die Person, die bestellt, ohne zu bezahlen, kreditwürdig ist und ihre Bestellung erhält. Die Identitätsprüfung mithilfe der E-ID ermöglicht es nicht, die Adresse oder Informationen über die Kreditwürdigkeit der betreffenden Person zu erhalten. Die Abfrage der in der E-ID enthaltenen persönlichen Daten erhöht nicht automatisch die Vertrauenswürdigkeit einer Bestellung auf Rechnung.

Abs. 2

Gemäss Absatz 2 veröffentlicht das BIT im Vertrauensregister eine Liste von Fällen der Identifizierung mittels E-ID, die gegen die Anforderungen von Absatz 1 verstossen. Dabei handelt es sich um eine wesentliche Sicherheitsmassnahme, die dazu dient, künftige Verstösse zu verhindern und die Nutzer über bekannte Verstösse zu informieren. Da das BIT nicht über die Kompetenz verfügt, solche Verletzungen aufzudecken, wird es tätig, wenn es von einem solchen Fall Kenntnis erhält. Es überprüft die Glaubwürdigkeit der Informationen, bevor es sie veröffentlicht. Ist eine Verifikatorin im Vertrauensregister eingetragen und erfüllt sie die Bedingungen von Absatz 1 nicht, kann das BIT zudem entscheiden, sie aus dem Vertrauensregister auszuschliessen.

Art. 23 Pflicht, die E-ID zu akzeptieren

Behörden und andere Stellen, die öffentliche Aufgaben erfüllen, müssen die staatliche E-ID akzeptieren, wenn sie die elektronische Identifizierung in Vollzug von Bundesrecht vornehmen. Demnach sind auch die Behörden von Kantonen und Gemeinden Adressaten dieser Norm, beispielsweise auch alle Betreibungsämter, wenn ein Auszug aus dem Betreibungsregister elektronisch bestellt und dabei die Identifikation mittels E-ID erfolgt (vgl. dazu auch die Erläuterungen zu Art. 33*a* Abs. 2bis SchKG). Dies ist angezeigt, weil die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet wird und damit vergleichbar ist mit Identitätskarte oder Pass in der physischen Welt, die auch bei jeder Identifizierung von allen Behörden akzeptiert wird. Die staatliche E-ID kann zusammen mit den bestehenden Mitteln für den Zugang zu E-Government-Diensten verwendet werden. Diese Verpflichtung gilt nur für Identifizierungsprozesse, bei denen ein persönliches Erscheinen und die Vorlage eines Identitätsdokuments erforderlich sind.

Artikel 23 unterstreicht die Bedeutung einer E-ID nach diesem Gesetz und deren Akzeptanz bei der Bevölkerung, wie sie sowohl in der Strategie Digitale Schweiz 2018–2022[39] als auch in der E-Government-Strategie Schweiz 2020–2023[40] definiert ist. Nicht zuletzt sollen so die vom Bund für die E-ID zu tätigenden Investitionen geschützt und eine breite Basis für die Anwendung der E-ID bei E-Government-Prozessen geschaffen werden. Davon profitieren nicht nur Bund, Kantone und Gemeinden, die damit mittelfristig Aufwände einsparen können, sondern auch alle Einwohnerinnen und Einwohner der Schweiz. Die Fragen im Zusammenhang mit der Verwendung der E-ID sowie die diesbezüglichen rechtlichen Folgen sind im Gesetzesentwurf nicht geregelt. Diese Fragen müssen für jeden Sektor einzeln geregelt werden. Der Gesetzesentwurf trägt insbesondere dem elektronischen Patientendossier sowie dem Bereich Schuldbetreibung und Konkurs Rechnung.

Art. 24 Alternative zum Vorweisen einer E-ID

Mit dem vorliegenden Artikel soll sichergestellt werden, dass die Inhaberinnen und Inhaber einer E-ID nicht verpflichtet sind, bei Interaktionen in der physischen Welt ihre E-ID vorzuweisen. Trotz der Vorteile der E-ID geht es nicht darum, die Möglichkeit auszuschliessen, (physische) Ausweise vorzuweisen. Wenn die Identifizierung einer Person in einem Prozess, der ihre Anwesenheit erfordert, anhand eines Ausweises erfolgen kann, darf das Vorweisen der E-ID (oder Bestandteilen davon) nur als Option angeboten werden.

Art. 25 Informationssystem zur Ausstellung und zum Widerruf der E-ID

Abs. 1

Fedpol betreibt ein Informationssystem, mit dem die Personendaten nach Artikel 13 bearbeitet werden. Das Informationssystem ermöglicht die Entgegennahme der Anträge der antragstellenden Personen und die Erfüllung der Aufgaben von fedpol bei der Ausstellung und dem Widerruf von E-ID.

Abs. 2

Das Informationssystem beinhaltet die Daten gemäss Artikel 14 Absatz 2 zu den beantragten und ausgestellten E-ID sowie die Daten zum Widerruf der E-ID. Weiter werden auch die Daten zum Ausstellungsverfahren gespeichert, die zu Statistik- und Supportzwecken sowie, bei Verdacht auf missbräuchlichen Bezug oder missbräuchliche Verwendung einer E-ID, zu Ermittlungszwecken erforderlich sind.

Abs. 3

Das Informationssystem kann für die Ausstellung einer E-ID auf die Daten nach Artikel 14 Absatz 1 und auf die folgenden Personenregister zugreifen, die auf Bundesebene geführt werden:

39 www.uvek.admin.ch > Kommunikation > Strategie «Digitale Schweiz»
40 www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Vorgaben > Strategien und Teilstrategien > SN001 – E-Government Strategie Schweiz

- das Informationssystem Ausweisschriften (ISA) nach Artikel 11 AwG;
- das Zentrale Migrationsinformationssystem (ZEMIS) gemäss den Artikeln 101 ff. AIG und der ZEMIS-Verordnung vom 12. April 2006[41];
- das elektronische Personenstandsregister (Infostar) gemäss den Artikel 39 ZGB und 6*a* der Zivilstandsverordnung vom 28. April 2004[42] (ZStV);
- das zentrale Versichertenregister der Zentralen Ausgleichsstelle der AHV (ZAS/UPI) nach Artikel 71 Absatz 4 des Bundesgesetzes vom 20. Dezember 1946[43] über die Alters- und Hinterlassenenversicherung (AHVG); das Informationssystem hat nur Zugriff auf den UPI-Teil des Registers, der für die Verwaltung der AHV-Nummer und den in Artikel 133bis Absatz 4 der Verordnung vom 31. Oktober 1947[44] über die Alters- und Hinterlassenenversicherung erwähnten Daten zuständig ist;
- das Informationssystem Ordipro des Eidgenössischen Departements für auswärtige Angelegenheiten nach Artikel 5 des Bundesgesetzes vom 18. Dezember 2020[45] über die Bearbeitung von Personendaten durch das Eidgenössische Departement für auswärtige Angelegenheiten und Artikel 2 der Ordipro-Verordnung vom 22. März 2019[46].

Somit kann fedpol seine Aufgaben bei der Ausstellung der E-ID automatisiert erfüllen. Auf dieser Grundlage kann es die Identität der antragstellenden Person überprüfen.

Abs. 4

Die via Schnittstellen aufgerufenen Daten werden weder dupliziert noch im Informationssystem von fedpol gespeichert. Sie werden direkt in den Registern des Bundes kontrolliert. Fedpol bearbeitet diese Daten ausschliesslich zum Zweck der Ausstellung und des Widerrufs der E-ID. Jeder andere Zweck der Bearbeitung dieser Daten ist somit ausgeschlossen.

Art. 26 Aufbewahrung und Vernichtung der Daten

Abs. 1

Dieser Artikel wurde eingeführt, um den Ergebnissen der Vernehmlassung Rechnung zu tragen. Einige Vernehmlassungsteilnehmende bedauerten, dass die Aufbewahrungsdauer und die Vernichtung der Daten im Vorentwurf nicht geregelt ist. Gemäss Artikel 6 Absatz 4 DSG werden Personendaten vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Diese Zwecke gehen aus den gesetzlichen Grundlagen hervor, die für die Datenbearbeitung gemäss den

41 SR **142.513**
42 SR **211.112.2**
43 SR **831.10**
44 SR **831.101**
45 SR **235.2**
46 SR **235.21**

Artikeln 14 und 25 dieses Gesetzesentwurfs vorgesehen sind. Artikel 26 sieht unterschiedliche Aufbewahrungsfristen für die drei Kategorien von Daten vor, unter Berücksichtigung der verschiedenen Bearbeitungszwecke der Daten.

Bst. a

Die von diesem Buchstaben betroffenen Daten werden höchstens 20 Jahre ab dem Antrags- oder Ausstellungsdatum der E-ID aufbewahrt. Trotz der verschiedenen Aufbewahrungsfristen für die in ISA, ZEMIS und Ordipro enthaltenen Daten gelten für die im Informationssystem von fedpol gespeicherten Daten von schweizerischen und ausländischen Staatsangehörigen die gleichen Fristen. Um den Prozess der Datenaufbewahrung zu vereinfachen, orientiert sich dieser Absatz an den Aufbewahrungsfristen für die Daten zu den Schweizer Identitätsausweisen gemäss Artikel 37 Absatz 1 der Ausweisverordnung vom 20. September 2002[47] (VAwG). So ist nur eine Aufbewahrungsfrist für die Daten von schweizerischen und ausländischen Staatsangehörigen vorgesehen.

Bst. b

Die Frist für die Aufbewahrung von Daten zum Ausstellungsprozess, die zur Untersuchung der Erschleichung einer E-ID erforderlich sind, einschliesslich der in Artikel 16 Absatz 3 genannten biometrischen Daten, ist aus Beweisgründen. gerechtfertigt. Es ist nicht davon auszugehen, dass eine Aufbewahrung dieser Daten über diese Frist hinaus nötig ist.

Abs. 2

Alle anderen Daten werden 90 Tage nach ihrer Eingabe im System vernichtet. Das Erfordernis soll sicherstellen, dass dieser Artikel für sämtliche Daten eine Aufbewahrungsfrist vorsieht. Die Daten, die nicht von Absatz 1 erfasst sind, werden nach Massgabe von Absatz 2 aufbewahrt.

Abs. 3

Absatz 1 gilt unter der Voraussetzung, dass Artikel 38 DSG und die Bestimmungen des Archivierungsgesetzes vom 26. Juni 1998[48] (BGA) eingehalten werden. Artikel 6 BGA bestimmt, dass die Daten, die nicht mehr benötigt werden, dem Bundesarchiv zur Übernahme angeboten werden. Daten, die das Bundesarchiv als nicht archivwürdig einstuft, werden vernichtet.

4. Abschnitt Zugänglichkeit für Menschen mit Behinderungen

Art. 27

Dieser Artikel wurde eingeführt, um den Vernehmlassungsergebnissen Rechnung zu tragen. Viele Vernehmlassungsteilnehmende bedauerten, dass der Vorentwurf keine

47 SR **143.11**
48 SR **152.1**

Bestimmungen zur Zugänglichkeit für Menschen mit Behinderungen vorsieht und haben diesbezüglich eine Reihe von Forderungen formuliert. Mit den Absätzen 1–3 sollen die Anforderungen des Behindertengleichstellungsgesetzes vom 13. Dezember 2002[49] (BehiG) und der Behindertengleichstellungsverordnung vom 17. November 2003[50] (BehiV) verdeutlicht und verstärkt werden.

Nach Artikel 14 Absatz 2 BehiG darf der Zugang zu Dienstleistungen, welche die Behörden im Internet anbieten, für sehbehinderte Personen nicht erschwert werden. Überdies bestimmt Artikel 10 Absatz 1 BehiV, dass «[d]ie Information sowie die Kommunikations- und Transaktionsdienstleistungen über das Internet […] für Sprach-, Hör- und Sehbehinderte sowie motorisch Behinderte zugänglich sein [müssen]».

Die Absätze 1 bis 3 von Artikel 27 orientieren sich an den Anforderungen von Artikel 10 Absatz 1 BehiV, wobei besonders aufgeführt wird, welche Bestandteile der Infrastruktur den Menschen mit Behinderungen zugänglich gemacht werden müssen. Die Anforderungen der BehiV sind auf die Anwendungen nach den Artikeln 7 und 8 nicht anwendbar, weil es da nicht um Dienstleistungen geht, die im Internet angeboten werden. Die Absätze 1 bis 3 sollen den Anwendungsbereich der Anforderungen der BehiV erweitern und diese gleichzeitig auf Gesetzesstufe verankern.

Abs. 1–3

Mit Absatz 1 soll gewährleistet werden, dass Menschen mit Behinderungen die E-ID beziehen können. Gemäss diesem Absatz muss fedpol sicherstellen, dass das Verfahren zum Bezug der E-ID den Standards zur Zugänglichkeit für Menschen mit Behinderungen entsprechen.

Absatz 2 sieht ebenfalls die Umsetzung der Zugänglichkeit für Menschen mit Behinderungen zu den vom Bund bereitgestellten Anwendungen vor, um die Verwendung der E-ID und anderer elektronischer Nachweise, wie der Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen (Art. 7) und der Anwendung zur Prüfung von elektronischen Nachweisen (Art. 8), zu erleichtern.

Zudem müssen die Standards zur Zugänglichkeit für Menschen mit Behinderungen beim Bezug und der Verwendung anderer elektronischer Nachweise eingehalten werden (Abs. 3). Die Bundes- und Kantonsbehörden, die die Vertrauensinfrastruktur nutzen, um elektronische Nachweise auszustellen und zu verifizieren, müssen bei diesen Verfahren die genannten Standards einhalten.

Abs. 4

Der Bundesrat wird ermächtigt, die Massnahmen zu regeln, die fedpol, das BIT und die Behörden ergreifen müssen, um den Zugang in den Fällen gemäss den Absätzen 1–3 zu gewährleisten. Er kann insbesondere spezifische Kommunikationsmassnahmen vorsehen und in diesem Bereich anerkannte technische Normen für verbindlich erklären. Zudem kann er regelmässige Kontrollen und Aktualisierungen verlangen. Der Bundesrat konsultiert bei der Erarbeitung der einschlägigen

[49] SR **151.3**
[50] SR **153.31**

Bestimmungen die Fachorganisationen und das Eidgenössische Büro für die Gleichstellung von Menschen mit Behinderungen.

5. Abschnitt Support

Art. 28

Die im Vorentwurf vorgesehenen Anforderungen an den Support wurden überarbeitet, um den Ergebnissen der Vernehmlassung Rechnung zu tragen. Einige Vernehmlassungsteilnehmende kritisierten, dass der Vorentwurf die Kantone beauftragt, Unterstützungsdienste vor Ort bereitzustellen. Viele Teilnehmende waren der Ansicht, dass die Bundesverwaltung allen Nutzerinnen und Nutzern der Vertrauensinfrastruktur einen Support zur Verfügung stellen müsse. Mit dem Artikel 28 wird der Bund beauftragt, im Rahmen der Ausstellung der E-ID und der Nutzung der Vertrauensinfrastruktur einen Support bereitzustellen. Es soll ein First-Level-Support in den drei Landessprachen der Schweiz sowie in Englisch zur Verfügung gestellt werden. Dieser Support kann von den Bundes-, Kantons- und Gemeindebehörden sowie von natürlichen Personen in Anspruch genommen werden.

6. Abschnitt Technische Entwicklung

Art. 29

Abs. 1

Die technische Entwicklung schreitet rasch voran und wird sich auch nach dem Inkrafttreten dieses Gesetzes fortsetzen. Um sicherzustellen, dass dieser Entwicklung Rechnung getragen werden kann, überträgt Absatz 1 dem Bundesrat die Kompetenz, auf Verordnungsstufe ergänzende Bestimmungen zu erlassen, damit die Vertrauensinfrastruktur an die technische Entwicklung angepasst werden kann und die in diesem Gesetz definierten Ziele weiterhin erreicht werden können.

Abs. 2

Aus verschiedenen Gründen kann für die ergänzenden Bestimmungen die Schaffung einer formellen gesetzlichen Grundlage erforderlich sein. Nach Artikel 34 Absatz 2 Buchstabe a DSG reicht es beispielsweise nicht, die Bearbeitung von besonders schützenswerten Personendaten in einer Verordnung zu regeln; hierfür ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. Mit der vorliegenden Gesetzesvorlage tritt die Verordnung des Bundesrates in drei Fällen ausser Kraft: wenn der Bundesrat zwei Jahre nach ihrem Inkrafttreten der Bundesversammlung keinen Entwurf einer gesetzlichen Grundlage unterbreitet hat; mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung; mit Inkrafttreten der gesetzlichen Grundlage.

7. Abschnitt Gebühren

Art. 30

Abs. 1

Bei den Ausstellerinnen und Verifikatorinnen werden für die Eintragung der Daten im Basisregister und im Vertrauensregister Gebühren erhoben.

Die Höhe der Gebühren, die im Gesetz nicht vorgesehen ist, wird auf Verordnungsstufe festgelegt. Sie dürfte im zwei- oder dreistelligen Frankenbereich liegen.

Abs. 2

In der Praxis hat sich etabliert, dass die Bundesbehörden von den Kantonsbehörden keine Gebühren für die Nutzung ihrer Infrastruktur erheben (und umgekehrt). Somit ist die Nutzung der Vertrauensinfrastruktur für die Gemeinden und Kantone kostenlos.

Abs. 3

Dieser Absatz präzisiert, dass für die Ausstellung der E-ID sowie für deren Nutzung, Überprüfung und Widerruf keine Gebühren erhoben werden, sofern dies online geschieht.

Auch die Verwendung der elektronischen Brieftasche des Bundes, die Konsultation des Basisregisters und die Verwendung des Vertrauensregisters sind kostenlos.

Durch eine weitgehende Gebührenbefreiung der Nutzer will dieser Absatz die Nutzung und Verbreitung der E-ID fördern. Der Bund hat ein grosses Interesse an einem möglichst verbreiteten Einsatz der E-ID, um den sicheren Datenaustausch mit Behörden und Privaten zu vereinfachen.

Abs. 4

Dieser Absatz wurde erarbeitet, um den Vernehmlassungsergebnissen Rechnung zu tragen. Die Kantone verlangten, dass im Gesetzesentwurf die Möglichkeit vorgesehen wird, für Dienstleistungen, die vor Ort erbracht werden, Gebühren zu erheben. Um dieser Forderung nachzukommen, ist vorgesehen, dass der Bundesrat auf Verordnungsstufe Bestimmungen erlässt, welche es der zuständigen Stelle ermöglicht, Gebühren für vor Ort erbrachte Leistungen zu erheben.

Abs. 5

Die Erhebung der Gebühren nach Artikel 46*a* RVOG regelt der Bundesrat in einer Verordnung.

8. Abschnitt Völkerrechtliche Verträge

Art. 31

In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern hat die Schweiz ein Interesse daran, die Möglichkeit zu schaffen, früher oder später in das europäische System für die Interoperabilität von elektronischen Identitäten eingebunden zu sein. Dafür braucht es ein internationales Abkommen. Dieser Artikel ermächtigt den Bundesrat, völkerrechtliche Verträge abzuschliessen, um die Verwendung und Anerkennung der E-ID auf internationaler Ebene zu erleichtern. Zudem kann er die erforderlichen Ausführungsvorschriften erlassen. Mit einem solchen Vertrag kann künftig die gegenseitige Anerkennung des schweizerischen Identifizierungssystems und derjenigen, die gemäss der eIDAS-Verordnung notifiziert oder von bestimmten EU-Mitgliedstaaten oder Drittstaaten eingeführt wurden, sichergestellt werden.

9. Abschnitt Schlussbestimmungen

Art. 32 Ausführungsbestimmungen

Die Ausführungsbestimmungen dieses Gesetzes regeln die Umsetzung der technischen und organisatorischen Aspekte der Übermittlung elektronischer Nachweise sowie die Funktionsweise der Bestandteile der Vertrauensinfrastruktur. Dabei soll insbesondere Folgendes geregelt werden: das Format der elektronischen Nachweise; die Standards und Protokolle für die Kommunikationsvorgänge beim Ausstellen und Vorweisen elektronischer Nachweise; die Bestandteile und die Funktionsweise des Basisregisters, des Systems zur Bestätigung von Identifikatoren, der Anwendung zur Aufbewahrung und zum Vorweisen von elektronischen Nachweisen und des Systems für Sicherungskopien; die Nachweise, die bei der Aufnahme in das System zur Bestätigung von Identifikatoren vorgelegt werden müssen; die technischen und organisatorischen Massnahmen für die Datensicherheit und den Datenschutz beim Betrieb und der Nutzung der Vertrauensinfrastruktur; die Schnittstellen sowie Elemente und Funktionsweise des Informationssystems für die Ausstellung und den Widerruf von E-ID.

Art. 33 Änderung anderer Erlasse

Im Anhang zum Gesetzesentwurf wird die Änderung anderer Erlasse vorgeschlagen. Insbesondere wird fedpol ermächtigt, auf die Informationssysteme ISA, Infostar und ZEMIS zuzugreifen. Mit den vorgeschlagenen Änderungen wird auch die Verwendung der E-ID in bestimmten Bereichen, wie dem elektronischen Patientendossier sowie im Bereich Schuldbetreibung und Konkurs, exemplarisch geregelt.

Art. 34 Übergangsbestimmung

Abs. 1

Nach Artikel 23 müssen die Behörden oder andere Stellen, die öffentliche Aufgaben erfüllen, die E-ID akzeptieren, wenn sie beim Vollzug von Bundesrecht eine elektronische Identifizierung vornehmen. Dieser Absatz sieht eine Frist von zwei Jahren nach Inkrafttreten des Gesetzes vor, um diese Verpflichtung umzusetzen.

Abs. 2

Um die Sicherheit, die Qualität des Systems und die Verfügbarkeit der technischen Unterstützung bei der Einführung zu gewährleisten, kann der Bundesrat eine gestaffelte Bereitstellung der Vertrauensinfrastruktur und der E-ID während maximal zwei Jahren nach dem Inkrafttreten dieses Gesetzes vorsehen. Dies betrifft insbesondere die verschiedenen Funktionen im Zusammenhang mit der elektronischen Brieftasche, wie die Speicherung von mehrfachen E-ID auf verschiedenen Medien oder die Speicherung der E-ID in Brieftaschen von Drittanbieterinnen. Eine gestaffelte Einführung der E-ID erlaubt es, Massnahmen zu ergreifen, um auf eine kontrollierte und risikobasierte Weise den Vollbetrieb zu erreichen.

Der Bundesrat kann auch Massnahmen ergreifen, die eine qualitative und sichere Online-Ausstellung gewährleisten. Erfahrungen aus anderen Ländern haben gezeigt, dass in den ersten Monaten eine hohe Nachfrage herrscht, was den Support und den Betrieb unter Druck setzt. Um eine qualitativ hochwertige und sichere Einführung des Systems zu gewährleisten, könnte in den ersten Monaten eine Mengensteuerung der ausgegebenen E-IDs pro Tag eingeführt werden, was möglicherweise eine Wartezeit für die Antragstellenden mit sich bringt.

Der Bundesrat könnte auch einen Zeitplan vorsehen, damit die Behörden, die für die vor Ort Prüfung der Identität zuständig sind (Art. 16 Abs. 1 Bst. b), sich organisieren und diese neue Aufgabe übernehmen können, wie die Kantone es gewünscht haben (vgl. Kap. 6.2).

Art. 35 Referendum und Inkrafttreten

Wie jedes Bundesgesetz untersteht auch der Gesetzesentwurf dem fakultativen Referendum. Der Bundesrat bestimmt das Datum des Inkrafttretens.

Änderung anderer Erlasse

Vorbemerkung

Die Anforderungen an die Identifizierung und Authentifizierung für E-Government-Anwendungen werden im geltenden Recht, sofern erforderlich, auf Verordnungs- oder Weisungsebene geregelt. Verschiedene Verordnungen und Weisungen müssen deshalb im Hinblick auf die Umsetzung des E-ID-Gesetzes geändert werden. Dies erfolgt aber erst mit dem Erlass der Ausführungsbestimmungen zum E-Gesetz. Nachfolgend wird deshalb nur die Änderung anderer Bundesgesetze erläutert.

Nach einer Evaluation der verschiedenen Bereiche des Bundesrechts sieht es so aus, dass mit dem vorliegenden Gesetzesentwurf nur die unten aufgeführten Gesetze geändert werden müssen. Die Evaluation hat alle einschlägigen Bereiche des Bundesrechts berücksichtigt. Ausserdem wurden Gespräche mit den eidgenössischen Departementen geführt, die an einem Einsatz der E-ID interessiert sind. Es gibt wenige Bereiche, in denen das Bundesrecht eine Personenidentifikation vorschreibt. Im Übrigen will das Gesetz nicht sämtliche Bereiche regeln, in denen elektronische Nachweise eingesetzt werden könnten. Es will vielmehr die rechtlichen Grundlagen schaffen, die für die Verwendung der E-ID und die Nutzung der Vertrauensinfrastruktur erforderlich sind. Es wird Sache der zuständigen Behörden sein, bei Bedarf die nötigen Rechtsgrundlagen in Spezialgesetzen vorzusehen.

1. Bundesgesetz vom 20. Juni 2003[51] über das Informationssystem für den Ausländer- und den Asylbereich

Art. 9 Abs. 1 Bst. c Ziff. 7bis und 2 Bst. c Ziff. 3 (neu)

In Artikel 9 Absatz 1 werden die Behörden aufgezählt, denen das SEM die von ihm oder in seinem Auftrag im Informationssystem nach dem BGIAA bearbeiteten Daten des Ausländerbereichs durch ein Abrufverfahren zugänglich machen kann. Buchstabe c hält fest, zu welchen Zwecken den Bundesbehörden im Bereich der inneren Sicherheit Zugang zu den Daten gewährt werden darf. Diese Liste soll mit einem neuen Zweck ergänzt werden: der Erfüllung der Aufgaben, für die sie gemäss diesem Gesetz zuständig sind.

In Artikel 9 Absatz 2 werden die Behörden aufgezählt, denen das SEM die von ihm oder in seinem Auftrag im Informationssystem nach dem BGIAA bearbeiteten Daten des Asylbereichs durch ein Abrufverfahren zugänglich machen kann. Buchstabe c hält fest, zu welchen Zwecken den Bundesbehörden im Bereich der inneren Sicherheit Zugang zu diesen Daten gewährt werden darf. Mit dem Gesetzesentwurf wird der Liste ein neuer Zweck angefügt: die Erfüllung der Aufgaben, die ihnen nach dem E-ID-Gesetz zukommen.

2. Ausweisgesetz vom 22. Juni 2001

Art. 1 Abs. 3 zweiter Satz

Grundsätzlich werden Schweizer Diplomaten- und Dienstpässe nur an Personen mit Schweizer Bürgerrecht abgegeben. Für gewisse Empfangsstaaten oder zur Übernahme von bestimmten Aufgaben im Interesse und im Auftrag der Schweiz ist es aus Sicherheitsgründen notwendig, auch an Personen ohne Schweizer Bürgerrecht einen Schweizer Diplomaten- oder Dienstpass auszustellen. Es soll verhindert werden, dass ausländischen Begleitpersonen von Schweizer Diplomaten oder anderen Angestellten einer Auslandsvertretung ernsthafte Nachteile drohen. Teilweise kann auch die

51 SR **142.51**

Anmeldung im Empfangsstaat und allenfalls die Ausstellung eines Visums nur erfolgen, wenn ein Schweizer Diplomaten- oder Dienstpass vorliegt. Die gesellschaftlichen Veränderungen im Bereich von Partnerschaften und hier insbesondere auch der Umstand, dass immer mehr Diplomatinnen und Diplomaten über fremdländische Ehe- oder Lebenspartner verfügen, hat die erwähnte Problematik zusätzlich verschärft. Weiter geht es auch darum, in Einzelfällen die Funktionsausübung ausländischer Mitarbeitenden zu erleichtern. Für gewisse Einsätze in Krisen- oder Kriegsregionen, die erhöhte Risiken für Leib und Leben mit sich bringen, ist das EDA darauf angewiesen, Spezialisten zu rekrutieren, die gegebenenfalls nicht über das Schweizer Bürgerrecht verfügen. Zu einer Schweizer Bürgerin oder zu einem Schweizer Bürger wird die Person trotzdem nicht. Im Pass wird auf der Personalienseite in der Rubrik Nationalität entsprechend auch der Heimatstaat der Person aufgeführt und der Heimatort durch «***» ersetzt.

Art. 11 Abs. 2 zweiter Satz

In Artikel 11 Absatz 2 wird aufgezählt, zu welchen Zwecken fedpol im Rahmen der Führung des ISA Daten bearbeiten darf. Es wird ein neuer Zweck der Datenbearbeitung hinzugefügt: die Erfüllung der Aufgaben nach dem E-ID-Gesetz.

3. Zivilgesetzbuch

Art. 43a Abs. 4 Ziff. 9

Artikel 43*a* ZGB regelt den Zugang im Abrufverfahren zu den elektronischen Registern zur Führung des Personenstandes. Die Auflistung der Stellen, die Zugriff auf Infostar haben, wird um fedpol erweitert.

4. Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs

Art. 33a Abs. 2bis

Gemäss Artikel 33*a* Absatz 1 SchKG können Eingaben bei den Betreibungs- und Konkursämtern und den Aufsichtsbehörden elektronisch eingereicht werden. Diese sind mit einer qualifizierten elektronischen Signatur zu versehen (Art. 33*a* Abs. 2 SchKG), womit die Eingabe eindeutig einer natürlichen Person zugeordnet werden kann. Da diese eindeutige Zuordnung auch mit dem Vorweisen einer E-ID sichergestellt werden kann, ist bei den Plattformen des Bundes oder eines Kantons auf das Anbringen einer qualifizierten elektronischen Signatur zu verzichten. Damit kann der Eingabeprozess für alle Beteiligten vereinfacht werden.

Der Bundesrat bestimmt, welche Plattformen dazu eingesetzt werden können. Dabei stehen beispielsweise die Plattformen nach dem Entwurf des Bundesgesetzes über die

Plattformen für die elektronische Kommunikation in der Justiz[52] oder die vom Staatssekretariat für Wirtschaft betriebene Plattform EasyGov[53].

5. Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier

Art. 7

Mit diesem Gesetzesentwurf wird der Begriff «elektronische Identität» in Artikel 7 des EPDG durch «elektronisches Identifikationsmittel» ersetzt. Der Begriff «elektronisches Identifikationsmittel» entspricht dem in diesem Artikel geregelten Konzept besser. Zudem sollen Verwechslungen mit dieser Vorlage vermieden werden, die den rechtlichen Rahmen für den staatlichen elektronischen Identitätsnachweis schafft. Bei letzterem handelt es sich um einen Identitätsnachweis einer Person in elektronischer Form und nicht um ein Identifikationsmittel für die Authentifizierung und den Zugang zu einem Dienst oder einer Anwendung. Aus Klarheitsgründen ist es angezeigt, eine begriffliche Unterscheidung zwischen den beiden Gesetzen beizubehalten und das EPDG zu ändern.

Art. 11 Bst. c

Nach dem heutigen System des EPDG werden die elektronischen Identifikationsmittel für den Zugang zum elektronischen Patientendossier von Privaten herausgegeben, die durch eine anerkannte Stelle zertifiziert sein müssen. Langfristig sollen auch diese Identifikationsmittel vom Bund herausgegeben werden. Damit soll dem politischen Willen des Souveräns mit der Ablehnung des E-ID-Gesetzes in der Volksabstimmung vom 7. März 2021 auch im Bereich des EPDG Nachachtung geschaffen werden, der diese Aufgabe nicht in den Händen der Privatwirtschaft sehen wollte.

Der Bund schafft mit den im EMBAG vorgesehenen Änderungen (siehe unten) die nötige Ausgangslage. Der Bund wird die Anforderungen nach der EPD-Gesetzgebung erfüllen müssen; eine Zertifizierung der zuständigen Bundesstelle ist dafür aber nicht erforderlich, weshalb darauf verzichtet werden soll. Da während einer gewissen Übergangszeit auch weiterhin private Identifikationsmittel für den Zugang zum elektronischen Patientendossier im Einsatz stehen werden, hält Artikel 11 Buchstabe c neu fest, dass private Herausgeber von Identifikationsmitteln weiterhin zertifiziert sein müssen.

6. Bundesgesetz vom 18. März 2016[54] über die elektronische Signatur

Art. 9 Abs. 4 und 4bis

52 BBl **2023** 679

53 Entspricht der zentralen elektronischen Plattform nach dem 4. Abschnitt des Entwurfs zum Bundesgesetz über die Entlastung der Unternehmen von Regulierungskosten (Unternehmensentlastungsgesetz, UEG), BBl **2023** 167; vgl. Botschaft vom 9. Dezember 2022 zum Bundesgesetz über die Entlastung der Unternehmen von Regulierungskosten (Unternehmensentlastungsgesetz, UEG), BBl **2023** 66, S. 34– 36.

54 SR **943.03**

Der zweite Satz von Absatz 4 wird aufgehoben. Im Ausgabeprozess für eine elektronische Signatureinheit ist die persönliche Vorsprache vorgeschrieben. Diese entfällt gemäss Absatz 4bis, wenn der Identitätsnachweis mit einem elektronischen Identifikationsmittel nach diesem Gesetz erbracht werden kann. Der Bundesrat kann in einer Verordnung vorsehen, dass die betreffende Person nicht persönlich erscheinen muss, wenn der Identitätsnachweis auf anderem Weg mit der erforderlichen Verlässlichkeit erbracht wird.

7. Bundesgesetz vom 17. März 2023 über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Dieser Gesetzesentwurf schafft den rechtlichen Rahmen für den staatlichen elektronischen Identitätsnachweis. Mit dem elektronischen Identitätsnachweis kann sich die Inhaberin oder der Inhaber identifizieren, aber nicht authentifizieren, um auf einen Online-Dienst oder eine Anwendung zuzugreifen. Aus diesem Grund wird mit diesem Gesetzesentwurf das zukünftige EMBAG geändert und ein Authentifizierungssystem als «IKT-Mittel» im Sinne von Artikel 11 Absätze 1–3 EMBAG eingeführt. Das System basiert auf der E-ID und kann Zugang zu einem Dienst oder einer Anwendung gewähren. Die E-ID wird in der Anwendung als Authentisierungsmittel ein Sicherheitsniveau vergleichbar mit «substanziell» gemäss eIDAS-Verordnung und Vertrauensstufe 3 des eCH-0170-Standards[55] erreichen.

Das System zur Authentifizierung natürlicher Personen (Authentifizierungsdienst der Schweizer Behörden, AGOV[56]) steht als IKT-Mittel auch den Kantonen und Gemeinden zur Verfügung. Zudem kann AGOV von Organisationen und Personen des öffentlichen oder privaten Rechts genutzt werden, soweit sie für den Vollzug von Bundesrecht zuständig sind.

Am Beispiel des elektronischen Patientendossiers wird nachfolgend exemplarisch dargestellt, wie die E-ID im Zusammenspiel mit AGOV künftig eingesetzt werden kann: Nach Erhalt einer E-ID kann eine Person AGOV nutzen, um auf ihr elektronisches Patientendossier zuzugreifen. Das heisst konkret, die Nutzerinnen und Nutzer des elektronischen Patientendossiers können die E-ID als digitalen Identitätsnachweis vorweisen und via AGOV wird daraus direkt ein Login-Vorgang für den Zugriff auf das elektronische Patientendossier abgeleitet.

Damit dies umsetzbar ist, müssen sich die Anbieterinnen des elektronischen Patientendossiers, die sogenannten Stammgemeinschaften, als Zielapplikation an AGOV anschliessen können (dies zum Beispiel mittels der Protokolle SAML [Security Assertion Markup Language] oder OIDC [OpenID Connect]). Die Kostenbeteiligung für die Nutzung von AGOV ist in Artikel 11 EMBAG geregelt und sieht eine anteilsmässige Übernahme der Aufwände vor, die durch die Nutzung verursacht wurden.

55 www.ech.ch > eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten V2.0
56 www.agov.ch

6 Auswirkungen

6.1 Auswirkungen auf den Bund

Damit die E-ID möglichst schnell zum Einsatz kommen kann, müssen parallel zum Gesetzgebungsprozess die technischen Vorarbeiten vorangetrieben werden. Die Erwartung in der Schweiz und die bisherige Kommunikation in Politik, Wirtschaft und Bevölkerung sind, dass der Bund mit Inkrafttreten des E-ID-Gesetzes technisch und operationell in der Lage ist, den Einwohnerinnen und Einwohnern der Schweiz sowie den Schweizerinnen und Schweizern im Ausland ihre digitale Identität und weitere digitale Nachweise (z. B. Strafregisterauszug) rasch und in einer hohen Qualität zur Verfügung zu stellen und die Bundesverwaltung nicht erst dann beginnt, an der technischen Lösung zu arbeiten. Um dies zu ermöglichen, wurden dem Parlament die für die Finanzierung der E-ID-Pilotprojekte und des Aufbaus der E-ID-Vertrauensinfrastruktur im Jahr 2023 zusätzlich notwendigen Mittel von insgesamt 6,6 Millionen Franken im Rahmen des Nachtrags I zum Voranschlag 2023 sowie ein Verpflichtungskredit für die Pilotierung und den Aufbau der E-ID-Vertrauensinfrastruktur von 40,4 Millionen Franken beantragt. Die Mittel für 2023 sowie der Verpflichtungskredit wurden am 1. Juni 2023 vom Parlament genehmigt.

Das E-ID-Vorhaben wird als Programm mit Projektkoordination gemäss Hermes geführt. Auftraggeber ist das BJ. Die Planung wird im Programmausschuss E-ID unter der Leitung des Direktors des BJ laufend abgestimmt und überwacht. Die Umsetzung in den einzelnen Projekten erfolgt agil. Gemäss Beschluss des Bundeskanzlers vom 17. April 2023 wird das E-ID-Vorhaben als sogenanntes DTI-Schlüsselprojekt der Bundesverwaltung geführt.[57]

Im Rahmen des E-ID-Vorhabens muss ein Informationssystem für die E-ID-Ausstellung sowie die E-ID-Vertrauensinfrastruktur aufgebaut, betrieben und weiterentwickelt werden. Insgesamt ergibt sich ein Ressourcenbedarf für den Aufbau, den Betrieb und die Weiterentwicklung von E-ID-Vertrauensinfrastruktur, E-ID-Ausstellung und die E-ID-Pilotprojekte von 2023–2028 von rund 181,9 Millionen Franken. Davon werden aus bestehenden Mitteln, dem Nachtrag I zum Voranschlag 2023 sowie dem Verpflichtungskredit für die Pilotierung und den Aufbau der E-ID-Vertrauensinfrastruktur rund 58,0 Millionen Franken finanziert. Für die überjährigen Verpflichtungen im Zusammenhang mit der Pilotierung und dem Aufbau der E-ID hat das Parlament mit dem Nachtrag I zum Voranschlag 2023 einen Verpflichtungskredit im Umfang von 40,4 Millionen bewilligt.

Der zusätzliche Ressourcenbedarf für den Abschluss des Aufbaus ab Mitte 2025 sowie für den Betrieb ab Anfang 2026 beträgt rund 123,9 Millionen Franken und ab 2029 jährlich rund 24,7 Millionen Franken.

Für den Abschluss des Aufbaus des E-ID Programms in den Jahren 2025–2026 ist ein Zusatzkredit im Umfang von 15,3 Millionen Franken erforderlich. Dieser ist einerseits notwendig, weil mit dem Antrag zum NK I im Frühling 2023 nur bis zum Zeitpunkt der Inbetriebnahme der E-ID Mittel anbegehrt wurden, womit der Zeitraum ab Mitte

57 www.bk.admin.ch > Dokumentation > Medienmitteilungen > Neue DTI-Schlüsselprojekte festgelegt

2025 bis Ende 2026 fehlt (7,7 Mio.). Andererseits wurden die Mittel für AGOV bezüglich dem Verpflichtungskredit beim NK I nicht vollständig berücksichtigt (7,6 Mio.).

Programm E-ID in Franken	VA2025	FP 2026	Total
E-ID-Ausstellungsinfrastruktur fedpol	6'701'500	965'700	**7'667'200**
AGOV/Pilotierung ePerso	5'600'000	2'000'000	**7'600'000**

Der beim fedpol benötigte Informatiksachaufwand wird für die öffentliche Ausschreibung der für die Online-Identitätsprüfung erforderlichen Technologie und Infrastruktur sowie die Entwicklung des Informationssystems der Staatlichen Identitätsstelle (SID) benötigt.

Zudem sind ab Mitte 2025 bis 2028 zwei weitere Verpflichtungskredite für 85,1 Millionen erforderlich (64,9 Millionen Franken für das BJ, 20,2 Millionen Franken für das fedpol). Sie werden nur solange benötigt, bis die bundesinternen Leistungserbringer in der Lage sind, den Betrieb des Systems selbst zu gewährleisten.

Neuer VK für das BJ	VA 2025	FP 2026	FP 2027	FP 2028	Total
Beratungs-/Drittleistungen (inkl. Kommunikation)	100'000	800'000	800'000	800'000	**2'500'000**
Audit/ISMS/Sicherheitszertifizierung	0	400'000	400'000	400'000	**1'200'000**
Betrieb BIT; Cloudinfrastruktur inkl. Lizenzkosten	3'100'000	3'100'000	3'100'000	3'100'000	**12'400'000**
Externe Mitarbeitende für den Betrieb	7'286'400	6'652'800	5'385'600	5'385'600	**24'710'400**
Externe Supportaufwände	2'595'000	2'880'000	810'000	810'000	**7'095'000**
Einmalige externe DL	3'000'000	5'000'000	5'000'000	4'000'000	**17'000'000**
Total	**16'081'400**	**18'832'800**	**15'495'600**	**14'495'600**	**64'905'400**

Für Beratungs- und übrige Drittleistungen sowie weitere Aufwendungen der E-ID-Fachstelle sind ab Mitte 2025 0,1 Millionen Franken und ab 2026 jährlich 0,8 Millionen Franken inkl. verschiedener Kommunikationsmassnahmen vorgesehen. Die externen Aufwände für Audit, Information Security Management System (ISMS) und Sicherheitszertifizierung betragen ab 2026 jährlich 0,4 Millionen Franken Franken. Der interne Sach- und Betriebsaufwand beträgt ab 2025 jährlich 3 Millionen Franken für den Betrieb der E-ID-Vertrauensinfrastruktur notwendigen Cloud-Infrastruktur. Investition zu Lasten des Anlagevermögens BIT sind nicht notwendig. Hinzu kommen jährlich 0,1 Millionen Franken an Lizenzkosten für das IT-Servicemanagement-Portal.

Externe Supportaufwände von 2,6 Millionen Franken für 2025, 2,9 Millionen Franken für 2026 sowie jährlich 0,8 Millionen Franken ab 2027 und Aufwände für externe Mitarbeitende für den Betrieb von 7,3 Millionen Franken für 2025, 6,7 Millionen Franken für 2026 und jährlich ab 2027 von 5,4 Millionen Franken bilden den letzten Teil an wiederkehrenden Betriebsaufwänden.

Bezüglich einmaligem externem Sach- und Betriebsaufwand sind für externe Dienstleistungen 2025 zusätzlich 3 Millionen Franken vorgesehen (ohne Support). Durch die wachsende Anzahl Teilnehmender am Ökosystem wie auch die technischen Entwicklungen im Ausland ist in den Jahren 2026 und 2027 noch ein signifikanter Investitionsschub zu erwarten, weshalb in diesen beiden Jahren 5 Millionen Franken und ab 2028 noch 4 Millionen Franken einmalig einzustellen sind.

Neuer VK für das fedpol	**VA 2025**	**FP 2026**	**FP 2027**	**FP 2028**	**Total**
Lizenzkosten	500'000	1'000'000	1'000'000	1'000'000	**3'500'000**
Betriebsaufwände	380'000	760'000	760'000	760'000	**2'660'000**
Wartung, Support und Weiterentwicklung	651'300	1'302'600	1'302'600	1'302'600	**4'559'100**
Externe Supportaufwände	1'584'000	3'168'000	3'168'000	1'584'000	**9'504'000**
Total	**3'115'300**	**6'230'600**	**6'230'600**	**4'646'600**	**20'223'100**

Die IT-Betriebsaufwendungen für die Jahre 2025–2028 unterteilen sich in Lizenzkosten für das System zur Online-Überprüfung der Identität eines Antragstellers, die auf 20% des Anschaffungspreises geschätzt werden, d.h. eine Million Franken. pro Jahr (die Hälfte davon im Jahr 2025). Die Betriebsaufwände für das Informationssystem des SID belaufen sich auf jährlich auf 0,76 Millionen Franken, wobei im Jahr 2025 nur die Hälfte berechnet wurde. Die Aufwände für Wartung, Support und Weiterentwicklung des Informationssystems, die auf 15 % der Entwicklungsaufwände geschätzt werden, entsprechen 1.3 Millionen Franken pro Jahr (im Jahr 2025 wiederum nur die Hälfte berechnet). Schliesslich betragen die einmaligen Aufwände für externe Supportstellen rund 1,6 Millionen Franken für 2025, je 3,2 Millionen Franken für 2026 und 2027 und 1,6 Millionen Franken für 2028). Diese externen Supportstellen werden ab 2029 nicht mehr erforderlich sein.

Bereits ab 2025 muss jede Stelle, die sich an die E-ID-Vertrauensinfrastruktur anbinden will (z.B. Finanzierung elektronischer Lehrfahrausweis durch die Kantone; heute Teil der Pilotierung), die Mittel für die Anbindung und deren Betrieb selber beantragen bzw. zur Verfügung stellen. Auch der Betrieb weiterer digitaler Nachweise ist durch die jeweiligen Betreiberinnen sicherzustellen.

Im erläuternden Bericht[58] zur Eröffnung der Vernehmlassung wurden in einer ersten Kostenschätzung (gestützt auf die Erfahrungen bei der Ausstellung des Covid-

58 www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > EJPD > Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Zertifikats) Projektaufwände zwischen 25 und 30 Millionen Franken und jährliche Betriebsaufwände zwischen 10 und 15 Millionen Franken ausgewiesen. Dabei wurde auch darauf hingewiesen, dass die Aufwände bei der Ausarbeitung der Botschaft genauer zu bestimmen sind. Auch die Form und die Dimensionen des Supports konnten erst jetzt aufgrund der ersten Erfahrungen in den Pilotprojekten genauer geschätzt werden.

Die hohen Aufwände für den technischen Support, welcher sowohl für die Vertrauensinfrastruktur als auch für die Herausgabe der E-ID gewährleistet werden muss, sind für die deutlich höheren Gesamtaufwände verantwortlich. Diese Aufwände waren im erläuternden Bericht zur Eröffnung der Vernehmlassung noch nicht berücksichtigt. Die Betriebsaufwände sind jeweils im Budgetprozess neu zu beurteilen und allenfalls anzupassen.

6.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Von verschiedener Seite wurde in der Vernehmlassung gefordert, dass der Überprüfungsprozess, der für Ausstellung der E-ID erforderlich ist, nicht nur über einen Online-Kanal, sondern auch mittels Vor-Ort-Prozess bei bestehenden Strukturen wie den Passbüros oder Migrationsämtern stattfinden soll. Damit wäre es für Interessierte möglich, den Besuch bei der Behörde in Kombination mit dem Antrag zur Ausstellung physischer Dokumente zu machen oder ausschliesslich zur Ausstellung der E-ID einen Vor-Ort-Termin wahrzunehmen.

Basierend auf internationalen Erfahrungen und anhand grober Schätzungen geht man von folgendem Mengengerüst aus: 50 Prozent der Personen, die für eine Ausweiserneuerung bei der Behörde vorbeikommen, werden sich zusätzlich für den Bezug der E-ID entscheiden; das sind rund 400 000 Fälle pro Jahr bei den Passbüros und etwa 130 000 Fälle bei den Migrationsämtern. Die Zahl der Personen, die explizit für die E-ID zu einer Behörde gehen, wird auf 1 Prozent aller potenziellen E-ID-Nutzerinnen und -Nutzer geschätzt. Sofern diese Möglichkeit bereits bei der Einführung der E-ID besteht, wird dies im ersten Jahr rund 28 000 Vor-Ort-Termine generieren, also anfänglich einen etwas höheren Anteil, später ab Jahr 4 etwa 1000 Fälle pro Jahr.

Die aktuellen Schätzungen des benötigten Aufwands pro Fall ergeben zusätzliche Aufwände von 15 Franken für die E-ID-Überprüfung im Zusammenhang mit dem Antrag auf ein Ausweisdokument. Es wird mit durchschnittlich zusätzlichen 7 Minuten bei der Behörde pro Fall gerechnet. Die Aufwände für eine Vor-Ort-Überprüfung nur zum Erhalt einer E-ID belaufen sich auf 28 Franken. Hier wird pro Fall mit durchschnittlich 14 Minuten gerechnet. Hochgerechnet auf die geschätzte Fallanzahl ergibt dies Aufwände von rund 8 Millionen Franken pro Jahr. Zum Vergleich: Die Aufwände beim Online-Kanal werden pro Fall im einstelligen Frankenbereich geschätzt. Dabei handelt es sich um vorläufige Kostenschätzungen, die möglicherweise, nach detaillierter Abstimmung mit den Kantonen, Änderungen erfahren werden. Sekundärkosten (Infrastrukturanpassungen von Gebäuden und Stationen, Personalführung) sind nicht Bestandteil der hier gemachten Berechnungen. Ebenfalls nicht vertieft

analysiert wurden Fragen hinsichtlich der Beschaffung und Finanzierung von allfällig erforderlichen Infrastrukturanpassungen.
Es soll den Kantonen überlassen werden, ob sie für ihre Dienstleistungen eine entsprechende Gebühr verlangen wollen, welche einheitlich vom Bundesrat festgelegt wird. Eine direkte Entschädigung durch den Bund ist nicht vorgesehen.

Nach mehreren Arbeitssitzungen mit Vertreterinnen und Vertretern von Passbüros und Migrationsämtern sowie einer Konsultation der Mitglieder des Verbands der Kantonalen Passstellen (VKP) und der Vereinigung der Kantonalen Migrationsbehörden (VKM) besteht das Hauptanliegen der Passbüros und Migrationsämter in der Kapazitätsbewältigung und den dafür benötigten Ressourcen und Infrastrukturen. Die durch die Kapazitätsbewältigung generierten Sekundärkosten (Infrastruktur der Stationen, Gebäude, Personalführung) wurden in den oben dargestellten Berechnungen nicht miteinbezogen. Infrastrukturanpassungen bringen nicht nur finanzielle Fragen mit sich, sondern stellen auch Zeitfragen zur Umsetzung (Tempo und Zyklen von Kredit- und Infrastrukturbeschaffungen). Dazu könnten die historisch bedingten «Hochjahre» (2025/2026 mit einer grossen Nachfrage nach Passerneuerungen), Änderungen aufgrund der avisierten Einführung von Identitätskarten mit Chip, eine erhöhte Nachfrage aufgrund erweiterter Sonderzeichen-Möglichkeiten sowie die Einführung des digitalen Führerausweises, die eine hohe Nachfrage nach E-ID mit sich bringen würde, zeitlich mit der Startphase der E-ID zusammenfallen.

Nebst der Koordination der oben genannten Aktivitäten können mehrere Ansätze verfolgt werden, um die Antragszahlen über die Zeit und gemäss Saisonalitäten besser zu verteilen: Die Ausstellung der E-ID vor Ort müsste nicht zwingend ab Beginn der E-ID möglich sein; die Anzahl verfügbarer Termine für die ausschliessliche Beantragung der E-ID könnte von jeder Behörde mit einer Quote begrenzt werden; eine gute Abstimmung zwischen Online-Kanal und den Verifikatorinnen vor Ort kann einem Überlauf entgegenwirken, der durch ein Quota-Maximum beim Online-Ausstellungsprozess entstehen könnte.

Als Hauptkanal für den Bezug einer E-ID wird der Online-Ausstellungsprozess dienen. Über Lenkungsmechanismen soll der Grossteil der Interessierten via Online-Kanal eine E-ID beziehen. Wenn die Interessierten für die Vor-Ort-Überprüfung eine Gebühr bezahlen müssten, wäre dies ein starker Faktor, um die Anfragen auf den kostenlosen Online-Kanal zu lenken. Aus Erfahrung ist bekannt, dass Behördendienstleistungen, die kostenlos sind, gerne in Anspruch genommen werden.

Die Aufwände für die Vor-Ort-Ausstellung könnten von den Kantonen oder den Antragstellenden selbst übernommen werden. Die Kantone profitieren direkt von der Bereitstellung und einem breiten Einsatz der E-ID. Sie können für diese Leistung aber auch Gebühren vorsehen. Der Bundesrat wird die Kantone auf dem Verordnungsweg ermächtigen, solche Gebühren zu erheben.

6.3 Auswirkungen auf die Volkswirtschaft

Die Digitalisierung schreitet voran. Immer mehr Geschäfte können online abgewickelt werden. Es ist immer weniger nötig, persönlich vorzusprechen. Es wird vermehrt erwartet, dass verschiedene Aufgaben elektronisch, vorzugsweise auf einem Smartphone, erledigt werden können. An Kommunikationsmitteln dafür mangelt es zwar nicht, es ist aber noch nicht möglich, elektronische Nachweise zu schaffen, zu verwalten und vorzuweisen, die einsatzfähig genug sind und von den meisten Anbieterinnen anerkannt werden. Mit der Vertrauensinfrastruktur des Bundes soll diese Lücke geschlossen werden. 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 von einem breiten Publikum akzeptiert und verwendet werden. Der elektronische Geschäftsverkehr im öffentlichen und im privaten Sektor kann, unter Beachtung der Anforderungen des DSG, effizienter und sicherer abgewickelt werden. Durch eine solche Infrastruktur können die Vernetzung zwischen den verschiedenen Akteuren und das Vertrauen in den elektronischen Geschäftsverkehr erhöht werden.

Einer der wesentlichen Vorteile der E-ID ist die Möglichkeit, eigene Daten einem Gegenüber im Internet vorweisen zu können. Die Inhaberinnen und Inhaber erhalten so nicht nur eine erhöhte Kontrolle über ihre Daten, sondern im Rahmen des elektronischen Geschäftsverkehrs auch mehr Verantwortung, namentlich hinsichtlich der Sorgfaltspflicht. Der Umfang der Verantwortung und deren Auswirkungen werden in einer Verordnung genauer definiert. Ausserdem erfordert der Besitz einer E-ID gewisse Kenntnisse über die Funktionsweise des eigenen Systems. Die öffentliche Debatte über den Gesetzesentwurf wird bereits in gewissem Masse zur Förderung der digitalen Kompetenz der Schweizer Bevölkerung in diesem Bereich beitragen.

6.4 Auswirkungen auf die Gesellschaft

Die sichere Identifizierung des Gegenübers bei einer elektronischen Transkation erschwert oder verhindert Missbräuche und fördert das Vertrauen. Missbräuche im Internet sind oft dadurch begründet, dass das Gegenüber nicht sicher identifiziert werden kann. Es ist heute weder möglich, Absender von Spams von verlässlichen Absendern zu unterscheiden, noch sie zur Verantwortung zu ziehen. Im Fall von Phishing geben sich die Absender von E-Mails als jemand aus, den sie nicht sind, beispielsweise als Bank der Empfängerin oder des Empfängers, und können damit grossen Schaden verursachen. Anerkannte elektronische Identifikationsmittel tragen in einer globalisierten und 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.

Technische Vorkehrungen sollen es ermöglichen, beim Vorweisen der E-ID oder eines anderen elektronischen Nachweises nicht immer alle enthaltenen Daten dem Gegenüber zu übermitteln und zum Beispiel zu verzichten. Es soll der Inhaberin oder

dem Inhaber der E-ID freistehen, alle oder nur einen Teil der darauf enthaltenen Informationen zu übermitteln. Damit kann die Privatsphäre besser geschützt werden, indem Informationen nicht mehr unbedingt mitgeteilt werden müssen.

Zudem sieht der Gesetzesentwurf Einschränkungen in Bezug auf die Verwendung der E-ID durch die Verifikatorinnen vor: Diese dürfen von der Inhaberin oder dem Inhaber einer E-ID nur unter bestimmten Voraussetzungen Daten verlangen. Damit will der Gesetzesentwurf eine ungerechtfertigte Nutzung der elektronischen Identifizierung durch die Verifikatorinnen einschränken.

6.5 Auswirkungen auf die Umwelt

Die Vorlage hat keine direkten Auswirkungen auf die Umwelt. Der Übergang von physischen zu elektronischen Transaktionen dürfte zu einer Einsparung von Ressourcen führen und sich somit positiv auf die Umwelt auswirken. Beispielsweise könnte eine Überlastung der Verkehrsinfrastruktur verhindert werden, weil es nicht mehr nötig ist, persönlich vorzusprechen.

Der Energiekonsum der Vertrauensinfrastruktur wird vergleichbar sein mit anderen Informatiksystemen, die der Bund bereits eingeführt hat. Für den Fall, dass die technische Umsetzungslösung auf einer Blockchaintechnologie basieren sollte, kann die Verwendung des für seinen grossen Energiekonsum bekannten Mechanismus «Proof of Work» für die Validierung der Blöcke bei der Bereitstellung der Vertrauensinfrastruktur als ausgeschlossen betrachtet werden.

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

Die Kompetenz zur Regelung der E-ID und der Vertrauensinfrastruktur ergibt sich aus den Artikeln 38 Absatz 1, 81 und 121 Absatz 1 BV. Nähere Erläuterungen dazu finden sich unter Abschnitt 5 (Ingress).

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Der Gesetzesentwurf ist mit den bestehenden internationalen Verpflichtungen vereinbar. Bei der Erarbeitung der Vorlage wurde darauf geachtet, dass die internationale Interoperabilität grundsätzlich möglich wäre. Falls zu einem späteren Zeitpunkt gewünscht, kann die E-ID internationale Anerkennung erlangen. Dazu wären internationale Abkommen notwendig.

7.3 Erlassform

Ausgehend von Gegenstand, Inhalt und Tragweite der Vorlage ist es aufgrund von Artikel 164 Absatz 1 BV notwendig, die Bestimmungen über elektronische Nachweise in der Form eines Bundesgesetzes zu erlassen.

Nach Artikel 163 Absatz 2 der Bundesverfassung und Artikel 25 Absatz 2 des Parlamentsgesetzes vom 13. Dezember 2002[59] hat der neue Erlass bezüglich Verpflichtungskredite die Form eines einfachen Bundesbeschlusses (der nicht dem Referendum unterliegt).

7.4 Unterstellung unter die Ausgabenbremse

Das Gesetz enthält keine Subventionsbestimmungen, weshalb es nicht der Ausgabenbremse zu unterstellen ist.

Nach Artikel 159 Absatz 3 Buchstabe b BV bedarf jedoch Artikel 1 Absatz 2 Buchstaben a und b des Bundesbeschlusses über die Verpflichtungskredite für den Aufbau und den Betrieb der E-ID der Zustimmung der Mehrheit der Mitglieder beider Räte, da beide Verpflichtungskredite einmalige Ausgaben von mehr als 20 Millionen Franken nach sich ziehen.

Der in Artikel 1 Absatz 1 des Bundesbeschlusses beantragte Zusatzkredit ist der Ausgabenbremse nicht zu unterstellen, weil der zugrundeliegende Verpflichtungskredit der Ausgabenbremse unterstand und der Zusatz für das einmalige Projekt für sich alleine den Schwellenwert von 20 Millionen Franken nicht übersteigt.

7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Die vorgesehene Aufgabenteilung und -erfüllung tangiert weder das Subsidiaritätsprinzip noch das Prinzip der fiskalischen Äquivalenz. Die finanziellen Auswirkungen der Vorlage auf den Bund sind höher als 10 Millionen Franken. Die finanziellen Auswirkungen auf die Kantone können noch nicht beziffert werden.

7.6 Einhaltung der Grundsätze des Subventionsgesetzes

Der Gesetzesentwurf sieht weder Finanzhilfen noch Abgeltungen vor.

59 RS **171.10**

7.7 Delegation von Rechtssetzungsbefugnissen

Der Gesetzesentwurf bewegt sich bewusst auf einem hohen Abstraktionsniveau (er ist in technologischer Hinsicht weitgehend neutral), um für künftige Veränderungen offen zu bleiben. Daher wird die Regelung einiger, teilweise auch bedeutender Fragen zur Ausgestaltung der Infrastruktur und des Leistungsumfangs der einzelnen Bestandteile der Infrastruktur sowie der E-ID wird an den Bundesrat delegiert.

7.8 Datenschutz

Die Regeln des Datenschutzrechts (DSG und die zugehörigen Verordnungen) gelten für alle. Die Einzelpersonen, die Ausstellerinnen und die Verifikatorinnen des privaten Sektors unterliegen den Bestimmungen, die für Private gelten. Der Bund (fedpol und andere Behörden), die Ausstellerinnen und Verifikatorinnen des öffentlichen Sektors unterliegen den Bestimmungen, die für Bundesorgane gelten. Im vorliegenden Gesetzesentwurf wird nicht auf die einschlägigen Bestimmungen des DSG verwiesen. Damit sollen Wiederholungen von gleichen Regelungen in unterschiedlichen Gesetzen vermieden werden. Dies insbesondere, um die Auslegung dieser Regelungen nicht zur erschweren.

Das Gesetz hat auch den Zweck, in seinem Regelungsbereich den Datenschutz zu fördern. Artikel 1 Absatz 2 Buchstabe a übernimmt im Übrigen den Wortlaut von Artikel 7 Absatz 2 DSG und präzisiert in den Ziffern 1–4, wie er im Kontext der E-ID umgesetzt werden wird. Es geht insbesondere darum, die Anforderungen der sechs inhaltlich identischen Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129) aufzunehmen, die nach der Ablehnung der früheren Vorlage in der Abstimmung vom 7. März 2021 von allen Fraktionen eingereicht wurden. Gemäss den Motionärinnen und Motionären muss die staatliche elektronische Identität gewissen Grundsätzen entsprechen: Es sollen insbesondere die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) eingehalten werden. In Artikel 1 Absatz 2 Buchstabe a werden diese Anforderungen als spezifische Zwecke formuliert, die im Rahmen des Schutzes der Personendaten zu erfüllen sind.

Artikel 1 Absatz 2 Buchstabe d des Gesetzesentwurfs soll ferner sicherstellen, dass die Ausgestaltung der E-ID und der Vertrauensinfrastruktur dem aktuellen Stand der Technik entspricht. Der Gesetzgeber strebt mit diesem Begriff ein hohes Niveau der Datensicherheit und des Datenschutzes dank fortschrittlichen Verfahren an. Artikel 1 Absatz 2 Buchstabe e präzisiert ausserdem, dass mit dem Gesetz gewährleistet werden soll, die technologische Entwicklung nicht unnötig einzuschränken. Der Gesetzesentwurf ist grundsätzlich technologieneutral; die Wahl der technischen Lösung wird nur geregelt, wenn dies für die Erreichung der gesetzgeberischen Ziele absolut erforderlich ist.

Die mit dem Gesetzesentwurf eingeführte Vertrauensinfrastruktur stützt sich auf die in den Artikeln 1 und 2 genannten Grundsätze. Die Hauptbestandteile dieser Infrastruktur sind im 2. Abschnitt geregelt: das Basisregister (Art. 2), das

Vertrauensregister (Art. 3), die Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen (Art. 7) und die Anwendung zur Prüfung von elektronischen Nachweisen (Art. 8). Das Basisregister und das Vertrauensregister beinhalten keine Daten zu den elektronischen Nachweisen. Das Basisregister enthält lediglich Daten zu deren Widerruf. Die Daten zu den Inhaberinnen und Inhabern der E-ID und den elektronischen Nachweisen werden ohne zwischengeschaltete Stelle ausschliesslich zwischen der Ausstellerin, der Inhaberin oder dem Inhaber und den Verifikatorinnen übermittelt. Die zentrale Idee hinter der Vertrauensinfrastruktur ist, ein System zu schaffen, in dem die Datenflüsse für alle Nutzerinnen und Nutzer direkt und transparent sind, in dem die Ausstellerinnen nicht wissen, wie die ausgestellten elektronischen Nachweise verwendet werden. Trotz dieser Einschränkungen für die Ausstellerinnen soll es ihnen möglich sein, Nachweise, die sie ausgestellt haben, zu widerrufen. Der Gesetzesentwurf sieht vor, dass die beim Aufrufen des Basis- und des Vertrauensregisters anfallenden Personendaten nur zu den in Artikel 57*l* Buchstabe b Ziffern 1-3 RVOG vorgesehenen Zwecke ausgewertet werden dürfen. Sie können ohne Personenbezug zu den Zwecken nach Artikel 57*l* Buchstabe b Ziffern 1-3 RVOG ausgewertet werden.

In Artikel 14 werden die Daten aufgeführt, die die E-ID enthält. Dabei handelt es sich um Personenidentifizierungsdaten (Abs 1) und Daten zur E-ID Daten (Abs. 2). Die Personenidentifizierungsdaten der Inhaberin oder des Inhabers umfassen: den amtlichen Namen, die Vornamen, das Geburtsdatum, das Geschlecht, den Heimatort, den Geburtsort, die Nationalität, das Gesichtsbild und die AHV-Nummer. Diese Daten sind in den amtlichen Registern des Staates verfügbar, auf die fedpol nach Artikel 25 Absatz 3 Zugriff hat. Neben den Personenidentifizierungsdaten enthält eine E-ID Daten, die von fedpol bei der Ausstellung der E-ID generiert werden. Dabei handelt es sich um die E-ID-Nummer, das Ausstellungsdatum, das Ablaufdatum, Angaben zum Ausweis, der im Ausstellungsprozess der E-ID verwendet wurde (einschliesslich Typ und Gültigkeitsdauer dieses Ausweises) und Angaben zum Ausstellungsprozess. Ferner kann die E-ID zusätzliche Daten enthalten, sofern sie im Ausweis der Inhaberin oder des Inhabers aufgeführt sind (z. B. Namen der gesetzlichen Vertretung, Allianznamen oder Künstlernamen).

Der vorliegende Gesetzesentwurf umfasst genaue Bestimmungen, die es fedpol erlauben, ein Informationssystem für die Identifizierung der antragstellenden Personen zu führen. In Artikel 25 Absatz 1 werden die Art, der Inhalt und der Zweck des Systems bestimmt. Nach Artikel 25 Absatz 2 enthält das System folgende Arten von Daten: die Daten zur E-ID gemäss Artikel 14 Absatz 2, die Daten zum Ausstellungsprozess (die zum Zweck des technischen Supports, der Statistik oder der Untersuchung erforderlich sind) sowie die Angaben zum Widerruf der E-ID.

Die Personenidentifizierungsdaten werden direkt in den Registern des Bundes abgefragt und nicht im Informationssystem von fedpol gespeichert (vgl. Art. 25 Abs. 4). In Artikel 25 Absatz 3 werden die Register des Bundes genannt, auf die fedpol Zugriff hat, damit es die Personendaten abgleichen kann. Das geplante System soll es fedpol ermöglichen, seine Aufgaben bei der Ausstellung und beim Widerruf der elektronischen Nachweise zu erfüllen.

In Artikel 16 Absatz 3 des Gesetzesentwurfs wird eine gesetzliche Grundlage im formellen Sinn geschaffen, die fedpol ermächtigt, für den Abgleich des Gesichts der

Person mit dem Gesichtsbild nach Artikel 14 Absatz 1 biometrische Daten zu erheben. Dieser Schritt ist nötig, um sicher zu gehen, dass das von der antragstellenden Person im Rahmen des Ausstellungsprozesses erfasste Gesichtsbild demjenigen entspricht, das in den Registern des Bundes (ISA, ZEMIS oder Ordipro) enthalten ist.

Artikel 22 führt wichtige Restriktionen ein, wenn die Verifikatorinnen in der E-ID enthaltene Personendaten bearbeiten. Die Verifikatorinnen dürfen diese Daten von den Inhaberinnen und Inhabern zur Überprüfung ihrer Identität oder eines Aspekts ihrer Identität anfordern, entweder aus Gründen einer benötigten Verlässlichkeit, oder weil es gesetzlich vorgeschrieben ist. Im Fall von Verstössen gegen diese Vorgaben wird das BIT die Verstösse im Vertrauensregister aufführen und kann fehlbare Verifikatorinnen aus dem Vertrauensregister ausschliessen.

Artikel 26 sieht für drei Arten von Daten, die im Informationssystem von fedpol enthalten sind, unterschiedliche Aufbewahrungsfristen vor. Die Daten zu den beantragten und ausgestellten E-ID und Angaben zum Widerruf der E-ID werden während 20 Jahren nach dem Antrags- oder Ausstellungsdatum aufbewahrt (Abs. 1 Bst. a), die Daten zum Ausstellungsprozess (einschliesslich der biometrischen Daten), die für die Untersuchung bei Verdacht auf Erschleichung einer E-ID erforderlich sind, während fünf Jahren nach dem Ablaufdatum der E-ID (Abs. 1 Bst. b). Alle anderen Daten werden 90 Tage nach ihrer Eingabe im System vernichtet (Abs. 2).

Ferner wird in Artikel 32 Buchstabe e auch die Kompetenz an den Bundesrat delegiert, in einer Verordnung die technischen und organisatorischen Massnahmen zu regeln, die zur Gewährleistung des Datenschutzes und der Datensicherheit beim Betrieb und der Nutzung der Vertrauensinfrastruktur erforderlich sind.