Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG)

StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.)

Änderung

BGBl. I Nr. 7/2008 idF BGBl. I Nr. 59/2008 (VFB) (NR: GP XXIII RV 290 AB 362 S. 41. BR: AB 7832 S. 751.)
BGBl. I Nr. 125/2009 (NR: GP XXIV RV 320 AB 419 S. 46. BR: 8199 AB 8216 S. 779.) [CELEX-Nr.: 32002L0091]
BGBl. I Nr. 111/2010 (NR: GP XXIV RV 981 AB 1026 S. 90. BR: 8437 AB 8439 S. 792.) [CELEX-Nr.: 32010L0012]
BGBl. I Nr. 83/2013 (NR: GP XXIV RV 2168 AB 2268 S. 200. BR: AB 8968 S. 820.) [CELEX-Nr.: 31995L0046]
BGBl. I Nr. 50/2016 idF BGBl. I Nr. 27/2019 (VFB) (NR: GP XXV RV 1145 AB 1184 S. 134. BR: 9594 AB 9607 S. 855.)
BGBl. I Nr. 40/2017 (NR: GP XXV RV 1457 AB 1569 S. 171. BR: 9747 AB 9752 S. 866.) [CELEX-Nr.: 32009L0031]
BGBl. I Nr. 121/2017 (NR: GP XXV IA 2227/A AB 1765 S. 190. BR: AB 9860 S. 871.)
BGBl. I Nr. 32/2018 (NR: GP XXVI RV 65 AB 97 S. 21. BR: 9947 AB 9956 S. 879.) [CELEX-Nr.: 32016L0680]
BGBl. I Nr. 104/2018 (NR: GP XXVI RV 381 AB 396 S. 55. BR: AB 10112 S. 887.)

Inhaltsverzeichnis

1. Abschnitt
Gegenstand und Ziele des Gesetzes

Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government Act – E-GovG)

⇐ Original version

as amended by:
(list of amendments published in the Federal Law Gazette)

⇐ amendment entailing the latest update of the present translation

Click here for checking the up-to-date list of amendments in the Austrian Legal Information System.

Table of contents

Part I
Object and aims of the act

2. Abschnitt
Eindeutige Identifikation und die Funktion E-ID

3. Abschnitt
Verwendung der Funktion E-ID im privaten Bereich oder bei Anwendungen im Ausland

4. Abschnitt
Elektronischer Datennachweis

Part II
Unique identification and the eID function

Part III
Use of the eID function in the private sector or abroad

Part IV
Electronic validation of data

1. Abschnitt

Gegenstand und Ziele des Gesetzes

§ 1. (1) Dieses Bundesgesetz dient der Förderung rechtserheblicher elektronischer Kommunikation. Der elektronische Verkehr mit öffentlichen Stellen soll unter Berücksichtigung grundsätzlicher Wahlfreiheit zwischen Kommunikationsarten für Anbringen an diese Stellen erleichtert werden.

(2) Gegen Gefahren, die mit einem verstärkten Einsatz der automationsunterstützten Datenverarbeitung zur Erreichung der in Abs. 1 genannten Ziele verbunden sind, sollen zur Verbesserung des Rechtsschutzes besondere technische Mittel geschaffen werden, die dort einzusetzen sind, wo nicht durch andere Vorkehrungen bereits ausreichender Schutz bewirkt wird.

Part I

Object and aims of the act

§ 1. (1) The object of this Federal Act is to promote legally relevant electronic communication. Electronic communications with public bodies are to be facilitated, having regard to the principle of freedom to choose between different means of communication when making submissions to such bodies.

(2) In order to improve legal protection, specific technical means shall be created to counter the risks associated with an increased use of automated data processing for the purposes of achieving the aims set out in subparagraph 1 and implemented where other precautions do not already provide adequate protection.

Recht auf elektronischen Verkehr

§ 1a. (1) Jedermann hat in den Angelegenheiten, die in Gesetzgebung Bundessache sind, das Recht auf elektronischen Verkehr mit den Gerichten und Verwaltungsbehörden. Ausgenommen sind Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden. Personen in gerichtlich, finanzstrafbehördlich oder gemäß § 53d des Verwaltungsstrafgesetzes 1991, BGBl. Nr. 52/1991, verwaltungsbehördlich angeordnetem Freiheitsentzug können dieses Recht nur nach Maßgabe der diesbezüglich in den Vollzugseinrichtungen vorhandenen technischen und organisatorischen Gegebenheiten ausüben, sofern dies vollzugsrechtlich zulässig ist und dadurch keine Gefährdung der Sicherheit und Ordnung zu erwarten ist.

(2) Etwaige technische Voraussetzungen oder organisatorische Beschränkungen des elektronischen Verkehrs sowie der Zeitpunkt der Aufnahme des elektronischen Verkehrs sind im Internet bekanntzumachen.

Teilnahme an der elektronischen Zustellung durch Unternehmen

§ 1b. (1) Unternehmen im Sinne des § 3 Z 20 des Bundesgesetzes über die Bundesstatistik (Bundesstatistikgesetz 2000), BGBl. I Nr. 193/1999, haben an der elektronischen Zustellung teilzunehmen.

(2) Die Teilnahme an der elektronischen Zustellung ist dann unzumutbar, wenn das Unternehmen nicht über die dazu erforderlichen technischen Voraussetzungen oder über keinen Internet-Anschluss verfügt.

(3) Die Teilnahme ist längstens bis 31. Dezember 2019 auch unzumutbar, wenn das Unternehmen noch nicht Teilnehmer des Unternehmensserviceportals ist sowie bei Fehlen elektronischer Adressen zur Verständigung im Sinne des Zustellgesetzes.

(4) Unternehmen können der Teilnahme an der elektronischen Zustellung widersprechen. Dieser Widerspruch verliert mit 1. Jänner 2020 seine Wirksamkeit, ausgenommen für Unternehmen, die wegen Unterschreiten der Umsatzgrenze nicht zur Abgabe von Umsatzsteuervoranmeldungen verpflichtet sind.“

Right of electronic communications

§ 1a. (1) Everyone has the right of electronic communications with courts and administrative bodies in matters of federal legislation excluded matters which are not suitable to be provided electronically**.** Persons in judicial, financial criminal administrative or corresponding to § 53d Administrative Penal Act 1991, Federal Law Gazette No. 52/1991 administrative disposed imprisonment can only use this right with the proviso of the existing technical and organizational conditions in penitentiaries if this is permissible and thereby is not to be expected a danger of security and order.

(2) Possible technical requirements or organizational limitations of the electronic communications as well as the moment of the entry of the electronic communications shall be announced on the Internet.

Participation in electronic delivery by companies

§ 1b. (1) Companies corresponding to § 3 No. 20 of the federal act about federal statistics, Federal Law Gazette I No. 193/1999, shall participate in electronic delivery.

(2) Participation in electronic delivery is unacceptable if the company does not have the necessary technical requirements or no Internet connection.

(3) Participation is also unacceptable until no later than 31 December 2019 if a company is not yet a participant in the Business Service Portal and if a company does not have any electronic addresses for the purpose of notification as referred to in the Service of Documents Act.

(4) Companies can refuse participation in electronic delivery. Such refusal loses effect as of 1 January 2020, except with regard to companies that are not obligated to submit a preliminary VAT return because they do not reach the turnover threshold.

2. Abschnitt
Eindeutige Identifikation und die Funktion E-ID

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeutet

1. „Identität“: die Bezeichnung der Nämlichkeit von Betroffenen (Z 7) durch Merkmale, die geeignet sind, ihre Unterscheidbarkeit von anderen zu ermöglichen; solche Merkmale sind insbesondere der Name und das Geburtsdatum, aber auch etwa die Firma oder (alpha)nummerische Bezeichnungen;
2. „eindeutige Identität“: die Bezeichnung der Nämlichkeit eines Betroffenen (Z 7) durch ein oder mehrere Merkmale, wodurch die unverwechselbare Unterscheidung von allen anderen bewirkt wird;

(Anm.: Z 3 aufgehoben durch BGBl. I Nr. 7/2008)

4. „Eindeutige Identifikation“: elektronische Identifizierung gemäß Art. 3 Z 1 eIDAS-VO (Z 11);
5. „Authentizität“: die Echtheit einer Willenserklärung oder Handlung in dem Sinn, dass der vorgebliche Urheber auch ihr tatsächlicher Urheber ist;

(Anm.: Z 6 aufgehoben durch BGBl. I Nr. 50/2016)

7. „Betroffener“: jede natürliche Person, juristische Person sowie sonstige Personenmehrheit oder Einrichtung, der bei ihrer Teilnahme am Rechts- oder Wirtschaftsverkehr eine eigene Identität zukommt;
8. „Stammzahl“: eine einem Betroffenen zu dessen eindeutiger Identifikation zugeordnete Zahl, die auch für die Ableitung von bereichsspezifischen Personenkennzeichen (bPK) gemäß §§ 9 und 14 bestimmt ist.
9. „Stammzahlenregister“: ein Register, das die für die eindeutige Identifikation von Betroffenen verwendeten Stammzahlen enthält bzw. die technischen Komponenten zur Ableitung von Stammzahlen im Bedarfsfall besitzt;
10. „Elektronischer Identitätsnachweis (E-ID)“: eine logische Einheit, die unabhängig von ihrer technischen Umsetzung eine qualifizierte elektronische Signatur (Art. 3 Z 12 eIDAS-VO) mit einer Personenbindung

Part II
Unique identification and the eID function

Definitions

§ 2. For the purposes of this federal act, the following definitions shall apply:

1. “Identity”: designation of a specific person (No. 7) by means of data which are suitable to distinguish persons from each other, such as, in particular, name and date of birth but also, for example, company name or (alpha)numerical designations;
2. “Unique identity”: designation of a specific person (No. 7) by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects;

(Note: No. 3 deleted by Federal Law Gazette I No. 7/2008)

4. “Unique identification”: electronic identification pursuant to Art. 3 No. 1 of the eIDAS-Regulation (No. 11);
5. “Authenticity”: the genuine nature of a declaration of intent or act in the sense that the purported author of that statement or act is in fact the actual author;

(Note: No. 6 repealed by Federal Law Gazette I No. 50/2016)

7. “Data subject”: any natural or legal person or other association or institution having its own identity for the purposes of legal or economic relations;
8. “Source PIN”: a number which is attributable to a data subject to be unambiguously identified and which also serves as the basis for generating sector-specific personal identifiers pursuant to § 9 and § 14;
9. “Source PIN register”: a register used for the purpose of uniquely identifying data subjects and comprising the technical components used, where necessary, for the generation of source identification numbers;
10. “Electronic proof of identity (eID)”: a logical unit that, independent of its technical implementation combines a qualified electronic signature (Art. 3 No. 12 of the eIDAS Regulation) with an identity link (§ 4 (2)) and the associated security data and functions.

(§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen verbindet;

11. „eIDAS-VO“: Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 155 vom 14.06.2016 S. 44.

§ 2a. Die Begriffsbestimmungen des Art. 3 eIDAS-VO gelten auch für dieses Bundesgesetz.

Identität und Authentizität

§ 3. (1) Im elektronischen Verkehr mit Verantwortlichen des öffentlichen Bereichs im Sinne des Art. 4 Z 7 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1 (im Folgenden: DSGVO) in Verbindung mit § 26 Abs. 1 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, dürfen Zugriffsrechte auf personenbezogene Daten (Art. 4 Z 1 DSGVO), nur eingeräumt werden, wenn die eindeutige Identität desjenigen, der zugreifen will, und die Authentizität seines Ersuchens nachgewiesen sind. Dieser Nachweis muss in elektronisch prüfbarer Form erbracht werden.

(2) Im Übrigen darf eine Identifikation von Betroffenen im elektronischen Verkehr mit Verantwortlichen des öffentlichen Bereichs nur insoweit verlangt werden, als dies aus einem überwiegenden berechtigten Interesse des Verantwortlichen geboten ist, insbesondere weil dies eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist.

Die Funktion E-ID

§ 4. (1) Der E-ID dient dem Nachweis der eindeutigen Identität, weiterer Merkmale sowie des Bestehens einer Einzelvertretungsbefugnis eines Einschreiters und der Authentizität des elektronisch gestellten Anbringens in Verfahren, für die ein Verantwortlicher des öffentlichen Bereichs eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet hat.

(2) Die eindeutige Identifikation einer natürlichen Person, die rechtmäßige Inhaberin eines E-ID (im Folgenden: E-ID-Inhaber) ist, wird durch die

11. “eIDAS Regulation”: (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.08.2014, p. 73, in the version of adjustment OJ L 155, 14.06.2016, p. 44.

§ 2a. The definitions of Art. 3 of the eIDAS-Regulation shall apply also for this Federal Act.

Identity and authenticity

§ 3. (1) In the context of electronic communications with public-sector controllers within the meaning of Art. 4 No. 7 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1 (in the following referred to as the “General Data Protection Regulation”) in connection with § 26 (1) of the Data Protection Act, Federal Law Gazette I No. 165/1999, rights of access to personal data (Art. 4 No. 1 of the General Data Protection Act) may be granted only where the unique identity of the person desiring access and the authenticity of his request have been validated. Such validation must be provided in a form which can be verified electronically.

(2) Identification of a person may otherwise be requested in communications with public-sector controllers only insofar as this is necessary in an overriding legitimate interest of the controller, in particular, where it is an essential requirement for the performance of a task assigned to the controller by statute.

The eID function

§ 4. (1) The eID serves to validate the unique identity, further features and the existence of sole power of representation of a person making a submission and of the authenticity of a submission made electronically in procedures for which a public-sector controller has set up a technical environment in which the eID can be used.

(2) The unique identification of a natural person who is the lawful holder of an eID (in the following referred to as “eID holder”) shall be effected by way of an

Personenbindung bewirkt: Von der Stammzahlenregisterbehörde (§ 7) wird elektronisch signiert oder besiegelt bestätigt, dass dem E-ID-Inhaber ein oder mehrere bPK zur eindeutigen Identifikation zugeordnet ist oder sind. Sofern die Personenbindung den Vornamen, Familiennamen, oder das Geburtsdatum des E-ID-Inhabers enthält, bestätigt die Stammzahlenregisterbehörde mit ihrer elektronischen Signatur oder ihrem elektronischen Siegel die Richtigkeit der Zuordnung dieser personenbezogenen Daten zum E-ID-Inhaber. Sofern mit Einwilligung des Betroffenen weitere Merkmale in die Personenbindung eingefügt werden, dient die elektronische Signatur oder das elektronische Siegel der Stammzahlenregisterbehörde der Bestätigung der unversehrten Einfügung dieser Merkmale aus den von der Stammzahlenregisterbehörde herangezogenen Registern von Verantwortlichen des öffentlichen Bereichs. Hinsichtlich des Identitätsnachweises im Fall der Stellvertretung gilt § 5.

(3) Um die E-ID Funktion nutzen zu können, bedarf es der vorherigen Registrierung des E-ID-Werbers (§ 4a).

(4) Aufgrund der Identitätsdaten des E-ID-Werbers (§ 4b Z 1 bis 4 und 6) hat die Stammzahlenregisterbehörde die Stammzahl des E-ID-Werbers zu ermitteln und diese in verschlüsselter Form an den qualifizierten Vertrauensdiensteanbieter (VDA) gemäß Art. 3 Z 20 eIDAS-VO, der das qualifizierte Zertifikat für eine elektronische Signatur ausstellt, das mit der Personenbindung zum E-ID des E-ID-Werbers verbunden werden soll, zu übermitteln. Zudem hat die Stammzahlenregisterbehörde diesem VDA die personenbezogenen Daten gemäß § 4b Z 1 bis 4, 7, 10 und 11 des E-ID-Werbers sowie eine allfällige Beschränkung der Gültigkeitsdauer des Zertifikats gemäß § 4a Abs. 2 zu übermitteln. Die Stammzahlenregisterbehörde hat diesem weiters alle Änderungen der übermittelten personenbezogenen Daten, die ihr zur Kenntnis gelangen, bekanntzugeben. Der VDA hat der Stammzahlenregisterbehörde unverzüglich den Identitätscode der ausgestellten Zertifikate gemäß Anhang I lit. f eIDAS-VO zu übermitteln.

(5) Bei der Verwendung des E-ID im elektronischen Verkehr gemäß § 10 Abs. 1 ist durch die Stammzahlenregisterbehörde oder die in ihrem Auftrag tätige Behörde eine Personenbindung (Abs. 2), die ein oder mehrere bPK, Vorname, Familienname und Geburtsdatum zum E-ID-Inhaber enthält, zu erstellen, und an die betreffende Datenverarbeitung zu übermitteln. Zu diesem Zweck hat der qualifizierte VDA die verschlüsselte Stammzahl, Vorname, Familienname und Geburtsdatum der Stammzahlenregisterbehörde zur Verfügung zu stellen. Nach Maßgabe der technischen Möglichkeiten können mit Einwilligung des E-ID-Inhabers in die Personenbindung weitere Merkmale zu diesem aus für die

identity link: the Source PIN Register Authority (§ 7) shall confirm, by electronic signature or electronic seal, that the eID holder has been allocated one or several sector-specific personal identifiers for the purpose of unique identification. If the identity link contains the first name, family name or date of birth of the eID holder, the Source PIN Register Authority shall confirm, by its electronic signature or its electronic seal, the correctness of the allocation of these personal data to the eID holder. To the extent that, with the consent of the data subject, further data are included in the identity link, the electronic signature or the electronic seal of the Source PIN Register Authority serves the purpose of confirming that these data were taken from registers of public-sector controllers used by the Source PIN Register Authority and included with their integrity preserved. With respect to validation of identity in the event of representation, § 5 shall apply.

(3) To be able to use the eID function, eID applicants must first register (§ 4a).

(4) The Source PIN Register Authority shall determine the source PIN of the eID applicant on the basis of the identity data of the eID applicant (§ 4b Nos. 1 to 4 and 6) and shall send this source PIN in encrypted form to the qualified trust service provider (TSP) pursuant to Art. 3 No. 20 of the eIDAS Regulation who shall issue the qualified certificate for an electronic signature, which certificate is to be combined with the identity link to form the eID of the eID applicant. In addition, the Source PIN Register Authority shall send to this TSP the eID applicant's personal data pursuant to § 4b Nos. 1 to 4, 7, 10 and 11 and any limitation of the period of validity of the certificate pursuant to § 4a(2). Furthermore, the Source PIN Register Authority shall notify this TSP of any changes of the personal data sent, of which the Source PIN Register Authority has obtained knowledge. The TSP shall immediately send to the Source PIN Register Authority the identity code pursuant to Annex I letter f of the eIDAS Regulation of the certificates issued.

(5) When the eID is used in electronic communications pursuant to § 10 (1), the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (subparagraph 2) containing one or more sector-specific personal identifiers, the first name, family name and date of birth of the eID holder and send it to the relevant data processing system. For this purpose, the qualified TSP shall provide to the Source PIN Register Authority the encrypted source PIN, first name, family name and date of birth. In accordance with the technical possibilities, further data of the eID holder taken from registers of public-sector controllers which the

Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen Bereichs eingefügt werden.

(6) Nach Maßgabe der technischen Möglichkeiten kann der E-ID-Inhaber den Bestand weiterer Merkmale gemäß Abs. 5 letzter Satz einem Dritten gegenüber in vereinfachter Form nachweisen. Zu diesem Zweck können diese weiteren Merkmale für einen begrenzten Zeitraum zu seinem E-ID gespeichert werden. Ob und für welchen Zeitraum dies für ein bestimmtes Merkmal zulässig ist, hat jener Verantwortliche des öffentlichen Bereichs festzulegen, der das Register führt, aus dem die Stammzahlenregisterbehörde dieses Merkmal bezogen hat.

(7) Die Authentizität eines mit Hilfe des E-ID gestellten Anbringens wird durch die in dem E-ID enthaltene elektronische Signatur nachgewiesen.

(8) Die näheren Regelungen zu den Abs. 1 bis 7 sind, soweit erforderlich, durch Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort im Einvernehmen mit dem Bundesminister für Inneres sowie den allfällig sonst zuständigen Bundesministern zu erlassen. Vor Erlassung der Verordnung sind die Länder und die Gemeinden, letztere vertreten durch den Österreichischen Gemeindebund und den Österreichischen Städtebund, anzuhören.

Registrierung und Widerruf des E-ID

§ 4a. (1) Die Registrierung der Funktion E-ID ist für Staatsbürger ab dem vollendeten 14. Lebensjahr im Rahmen der Beantragung eines Reisedokumentes nach dem Passgesetz 1992, BGBl. Nr. 839/1992, ausgenommen eines Reisepasses gemäß § 4a des Passgesetzes 1992, von Amts wegen durch die Passbehörde oder durch eine gemäß § 16 Abs. 3 des Passgesetzes 1992 ermächtigte Gemeinde vorzunehmen, sofern der Betroffene dieser nicht ausdrücklich widerspricht. Darüber hinaus können sie die Registrierung eines E-ID bei der Passbehörde, einer gemäß § 16 Abs. 3 des Passgesetzes 1992 ermächtigten Gemeinde oder der Landespolizeidirektion verlangen. Soweit die Registrierung nicht im Rahmen der Beantragung eines Reisedokumentes erfolgt, ist die Behörde örtlich zuständig, bei der das Verlangen auf Registrierung des E-ID gestellt wird. Im Einvernehmen mit dem Bundesminister für Inneres können auch andere geeignete Behörden die Registrierung des E-ID vornehmen. Der Bundesminister für Inneres hat diese Behörden im Internet zu veröffentlichen.

(2) Die sachliche Zuständigkeit zur Registrierung des E-ID für Fremde kommt der Landespolizeidirektion zu. Örtlich zuständig ist die Landespolizeidirektion, bei der das Verlangen auf Registrierung des E-ID gestellt wird. Bei Fremden ist eine Registrierung nur dann vorzunehmen, sofern sie über einen ausreichenden Bezug

Source PIN Register Authority can access can be included in the identity link with the consent of the eID holder.

(6) In accordance with the technical possibilities, the eID holder can prove the existence of further data pursuant to subparagraph 5 last sentence to a third party in simplified form. For this purpose, these further data can be stored on the eID holder's eID for a limited period. The public-sector controller keeping the register from which the Source PIN Register Authority took the data shall determine whether and for which period this is permissible for certain data.

(7) The authenticity of a submission made using the eID shall be validated by the electronic signature contained in the eID.

(8) Where necessary, detailed rules on subparagraphs 1 to 7 shall be laid down in a regulation of the Federal Minister of Digital and Economic Affairs adopted with the consent of the Federal Minister of the Interior and any other competent Federal Ministers. The provinces and the municipalities, the latter represented by the Austrian Association of Municipalities and the Austrian Association of Cities and Towns, shall be consulted prior to adoption of that regulation.

Registration and revocation of the eID

§ 4a. (1) The passport authority or a municipal authority authorised pursuant to § 16 (3) of the Passport Act 1992 shall automatically register the eID function for citizens from the age of 14 during the application process for a travel document pursuant to the Passport Act 1992, Federal Law Gazette No. 839/1992, with the exception of a passport pursuant to § 4a of the Passport Act 1992, unless the data subject expressly objects to registration. In addition, citizens from the age of 14 can request registration of an eID from the passport authority, a municipal authority pursuant to § 16 (3) of the Passport Act 1992 or a provincial police directorate. Unless the eID is registered during the application process for a travel document, the authority with which the request for registration of an eID was filed has territorial jurisdiction. With the consent of the Federal Minister of the Interior, other appropriate authorities can also register an eID. The Federal Minister of the Interior shall publish these authorities on the Internet.

(2) The provincial police directorates have subject-matter jurisdiction over the registration of eIDs for foreigners. Territorial jurisdiction lies with the provincial police directorate with which the request for registration of an eID was filed. For foreigners, an eID may be registered only if they have sufficient relations to Austria

zum Inland verfügen und das 14. Lebensjahr vollendet haben. Insbesondere ist hiefür ein Nachweis über Wohnsitz, Beschäftigungsverhältnis oder Geschäftstätigkeit im Inland erforderlich. Für Fremde, die im Inland internationalen Schutz beantragt haben, ist die Registrierung erst nach Zuerkennung des Status des Asylberechtigten oder des subsidiär Schutzberechtigten oder der Erteilung eines sonstigen Aufenthaltsrechts zulässig. Für Fremde ohne Hauptwohnsitz im Bundesgebiet darf das qualifizierte Zertifikat für elektronische Signaturen gemäß Art. 3 Z 15 eIDAS-VO ab dem Zeitpunkt der Registrierung maximal drei Jahre gültig sein. Abs. 1 vorletzter und letzter Satz gelten für Fremde sinngemäß.

(3) Soweit Inhaber eines inländischen Reisedokumentes den Behörden bereits vorweg in der Verordnung gemäß Abs. 6 näher bestimmte personenbezogene Daten zur Verfügung stellen, dürfen sie diese zur Weiterverarbeitung zum Zweck der Registrierung eines E-ID für 30 Tage speichern. Erfolgt innerhalb dieses Zeitraums keine Registrierung des E-ID, sind diese personenbezogenen Daten zu löschen.

(4) Die Registrierung des E-ID ist nur zulässig, sofern die Identität des Betroffenen eindeutig festgestellt wurde. Zur Überprüfung der Identität und der vorgelegten Dokumente ist die Behörde ermächtigt, Informationen über diese personenbezogenen Daten und Dokumente aus Datenverarbeitungen von Sicherheits-, Personenstands- und Staatsbürgerschaftsbehörden im Datenfernverkehr einzuholen. Kann die Identität des E-ID-Werbers bei den Behörden gemäß Abs. 1 und 2 nicht eindeutig festgestellt werden, obliegt das weitere Verfahren zur eindeutigen Feststellung der Identität der Landespolizeidirektion.

(5) Die Aussetzung oder der Widerruf des E-ID erfolgt durch die Aussetzung oder den Widerruf des mit dem E-ID verbundenen qualifizierten Zertifikats beim VDA gemäß § 6 des Signatur- und Vertrauensdienstegesetzes – SVG, BGBl. I Nr. 50/2016, oder Art. 24 Abs. 3 eIDAS-VO. Dieser hat die Information über die Aussetzung oder den Widerruf der jeweils zuständigen Behörde gemäß Abs. 1 und 2 im Wege des Betreibers der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 zur weiteren Verarbeitung zu übermitteln. Die Behörden gemäß Abs. 1 und 2 haben die Aussetzung oder den Widerruf des E-ID zu veranlassen, wenn ihnen bekannt wird, dass der Inhaber des E-ID verstorben ist, die Gefahr missbräuchlicher Verwendung droht, der E-ID-Inhaber dies verlangt oder wenn der Behörde Tatsachen bekannt werden, die berechtigte Zweifel an der Identität des Betroffenen aufkommen lassen.

(6) Der Bundesminister für Inneres hat im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort nähere Bestimmungen

and are older than 14. In particular, proof of residence, employment or business activities in Austria is required for this purpose. In the case of foreigners who applied for international protection in Austria, registration is permissible only after they were granted asylum status or subsidiary protection status or another right of residence. In the case of foreigners who do not have their principal place of residence in the federal territory, the qualified certificate for electronic signatures pursuant to Art. 3 No. 15 of the eIDAS Regulation may be valid for a maximum of three years from the time of registration. Subparagraph 1 penultimate and last sentences shall apply to foreigners mutatis mutandis.

(3) To the extent that holders of an Austrian travel document provide to the authorities personal data, specified in more detail in the regulation pursuant to subparagraph 6, in advance, the authorities may store these data for further processing for 30 days for the purpose of registration of an eID. If no eID is registered within this period, these personal data must be deleted.

(4) Registration of an eID is permissible only if the data subject has been uniquely identified. To verify the identity and the documents provided, the authority is authorised to obtain, via electronic communications, information on these personal data and documents from data processing systems of security authorities, civil status authorities and nationality authorities. If an eID applicant cannot be uniquely identified by the authorities pursuant to subparagraphs 1 and 2, the provincial police directorates are responsible for the further procedures for unique identification.

(5) An eID is suspended or revoked by having the qualified certificate linked with the eID suspended or revoked by the TSP pursuant to § 6 of the Signature and Trust Services Act, Federal Law Gazette I No. 50/2016, or Art. 24 (3) of the eIDAS Regulation. The TSP shall send the information on the suspension or revocation to the relevant competent authority pursuant to subparagraphs 1 and 2 through the operator of the data processing system pursuant to § 22b of the Passport Act 1992 for further processing. The authorities pursuant to subparagraphs 1 and 2 shall arrange for the suspension or revocation of the eID if they learn that the eID holder has died, if there is the risk of misuse, if the eID holder requests so or if the authority obtains knowledge of facts giving rise to justified doubts about the identity of the data subject.

(6) The Federal Minister of the Interior, with the consent of the Federal Minister of Digital and Economic Affairs, shall specify, by regulation, detailed

über die Vorgangsweise gemäß Abs. 1 bis 5 sowie für die Verlängerung der Gültigkeit eines E-ID durch Verordnung festzulegen.

Registrierungsdaten

§ 4b. Die mit der Registrierung des E-ID betrauten Behörden sind ermächtigt als Verantwortliche

1. den Namen,
2. das Geburtsdatum,
3. den Geburtsort,
4. das Geschlecht,
5. die Staatsangehörigkeit,
6. das bPK,
7. die bekanntgegebene Zustelladresse,
8. das Lichtbild,
9. das Registrierungsdatum,
10. soweit verfügbar die bekanntgegebene Telefonnummer eines Mobiltelefons,
11. soweit verfügbar die bekanntgegebene E-Mail-Adresse,
12. die Registrierungsbehörde und
13. den Identitätscode der ausgestellten Zertifikate gemäß § 4 Abs. 4

in der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 zu verarbeiten. Dabei ist eine Speicherung nur vorzunehmen, soweit die personenbezogenen Daten nicht bereits in dieser Datenverarbeitung, im Zentralen Melderegister oder dem Ergänzungsregister zur Verfügung stehen. Der Bundesminister für Inneres sowie die Stammzahlenregisterbehörde sind ermächtigt, diese personenbezogenen Daten zu Zwecken der Verwaltung des E-ID zu verarbeiten. Die Verarbeitung dieser personenbezogenen Daten zu anderen Zwecken als der Verwaltung des E-ID ist nur auf Grund besonderer gesetzlicher Anordnung zulässig.

E-ID und Stellvertretung

§ 5. (1) Für Zwecke des vertretungsweisen Handelns kann in die Personenbindung des Vertreters von der Stammzahlenregisterbehörde das Bestehen einer Einzelvertretungsbefugnis für die Vertretung von nicht-natürlichen Personen oder einer Vertretungsbefugnis für die Vertretung von natürlichen Personen eingefügt werden. Zu diesem Zweck kann die Stammzahlenregisterbehörde nach Maßgabe der technischen Möglichkeiten Angaben zu Vollmachtsverhältnissen in

provisions on the procedure pursuant to subparagraphs 1 to 5 and on the extension of the validity of an eID.

Registration data

§ 4b. The authorities entrusted with registering an eID, as controllers, are authorised to process

1. the names,
2. the date of birth,
3. the place of birth,
4. the sex,
5. the nationality,
6. the sector-specific personal identifier,
7. the address for service provided,
8. the photograph,
9. the date of registration,
10. if available, the telephone number of a mobile telephone provided,
11. if available, the email address provided,
12. the registering authority, and
13. the identity code of the certificate issued pursuant to § 4(4)

in the data processing system pursuant to § 22b of the Passport Act 1992. They may store these personal data only if these data are not yet available in this data processing system, the Central Register of Residents or the Supplementary Register. The Federal Minister of the Interior and the Source PIN Register Authority are authorised to process these personal data for purposes of administering the eID. Processing these personal data for purposes other than administering the eID is permissible only on the basis of special instructions laid down by law.

eID and representation

§ 5. (1) For the purposes of acting as a representative, the Source PIN Register Authority can include in the identity link of the representative the existence of sole power of representation in the case of representation of non-natural persons or power of representation in the case of representation of natural persons. For this purpose, the Source PIN Register Authority can use, in accordance with the technical possibilities, information on powers of attorney in data processing systems

Datenverarbeitungen anderer Verantwortlicher des öffentlichen Bereichs verwenden, sofern dies gesetzlich zulässig ist oder eine Einwilligung des Betroffenen besteht. Die Stammzahlenregisterbehörde kann außerdem auf Antrag des Vertreters das Bestehen eines Vertretungsverhältnisses mit allfälligen inhaltlichen und zeitlichen Beschränkungen speichern. Die Voraussetzungen und näheren Anforderungen des Antrags und der zu erbringenden Nachweise sind in der gemäß § 4 Abs. 8 zu erlassenden Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort festzulegen. Die Berechtigung zur Empfangnahme von Dokumenten gemäß § 35 Abs. 3 zweiter Satz des Zustellgesetzes – ZustG, BGBl. Nr. 200/1982, muss gesondert eingefügt werden.

(2) In den Fällen berufsmäßiger Parteienvertretung ist ein besonderer Vollmachtsnachweis nicht erforderlich, wenn die generelle Befugnis zur Vertretung aus der nach den berufsrechtlichen Vorschriften erfolgenden Anmerkung der Berufsberechtigung im Signaturzertifikat seines E-ID oder auf Grund von Datenverarbeitungen, die nach berufsrechtlichen Bestimmungen zu führen sind, ersichtlich ist. In diesen Fällen wird das Bestehen der berufsmäßigen Parteienvertretung von der Stammzahlenregisterbehörde gemäß Abs. 1 in die Personenbindung eingefügt. Die generelle Befugnis umfasst nicht die Berechtigung gemäß § 35 Abs. 3 zweiter Satz ZustG.

(3) Soweit diese Dienstleistung bei Behörden eingerichtet ist, können unabhängig von ihrer sachlichen und örtlichen Zuständigkeit hiezu eigens ermächtigte Organwalter für Betroffene auf deren Verlangen Verfahrenshandlungen in E-ID-tauglichen Verfahren setzen. Der Auftrag des Betroffenen ist bei der Behörde in geeigneter Form zu dokumentieren. Die Verfahrenshandlung wird mit Hilfe des E-ID des Organwalters gesetzt. Die generelle Befugnis des Organwalters zur Vornahme der Verfahrenshandlung für Betroffene muss aus dem Signaturzertifikat seines E-ID oder aus einer von der zuständigen Behörde geführten Datenverarbeitung ersichtlich sein. In diesen Fällen wird das Bestehen der Befugnis des Organwalters von der Stammzahlenregisterbehörde gemäß Abs. 1 in die Personenbindung eingefügt. Die generelle Befugnis umfasst nicht die Berechtigung gemäß § 35 Abs. 3 zweiter Satz ZustG und die Zustellungsvollmacht gemäß § 9 Abs. 1 ZustG.

(4) Wird das Bestehen einer Einzelvertretungsbefugnis in die Personenbindung (§ 4 Abs. 2) eingefügt, dient die elektronische Signatur oder das elektronische Siegel der Stammzahlenregisterbehörde der Bestätigung der unversehrten Einfügung der Einzelvertretungsbefugnis aus den von der Stammzahlenregisterbehörde herangezogenen Quellen. § 4 Abs. 5, § 14 Abs. 3 und

of other public-sector controllers if this is permissible by law or the data subject has consented. In addition, the Source PIN Register Authority, upon application of the representative, can store information on the existence of power of representation, including any relevant material or temporal limitations. The prerequisites and detailed requirements of the application and the proof to be submitted shall be specified in the regulation by the Federal Minister of Digital and Economic Affairs to be adopted pursuant to § 4 (8). The permission to receive documents pursuant to § 35 (3) second sentence of the Service of Documents Act, Federal Law Gazette No. 200/1982, must be entered separately.

(2) In cases of professional representation no particular proof of a power of attorney is required if the general authority to represent is evident from the notice of professional entitlement in the signature certificate of an eID made in accordance with professional regulations or on the basis of data processing systems to be operated in accordance with professional regulations. In these cases, the Source PIN Register Authority shall include the existence of professional representation in the identity link pursuant to subparagraph 1. The general authority does not include the permission according to § 35 (3) second sentence of the Service of Documents Act.

(3) Provided that such a service is offered by authorities, officials authorised especially for this purpose may, at a data subject's request, lodge applications for that data subject with all authorities, irrespective of their subject-matter or territorial jurisdiction, in procedures in which an eID may be used. The specific instruction issued by the citizen shall be documented and kept by the authority in an appropriate form. Applications shall be lodged using the eID of the official. The general competence of an official to lodge applications for citizens must be apparent from the signature certificate of the official's eID or from the data processing system operated by the competent authority. In these cases, the Source PIN Register Authority shall include the existence of the official's authority in the identity link pursuant to subparagraph 1. The general authority does not include the permission according to § 35 (3) second sentence of the Service of Documents Act and the authorisation for deliveries § 9 (1) of the Service of Documents Act).

(4) If the existence of sole power of representation is included in the identity link (§ 4 (2)), the electronic signature or the electronic seal of the Source PIN Register Authority serves the purpose of confirming that sole power of representation was included, with its integrity preserved, on the basis of sources used by the Source PIN Register Authority. § 4 (5), § 14 (3) and § 14a (2) shall

§ 14a Abs. 2 gelten für vertretungsweises Handeln in Bezug auf vertretene natürliche Personen sinngemäß. Für vertretene nicht-natürliche Personen hat die Stammzahlenregisterbehörde die Stammzahl bereitzustellen.

Stammzahl

§ 6. (1) Im E-ID erfolgt die eindeutige Identifikation von Betroffenen durch ihre Stammzahl.

(2) Für natürliche Personen, die im Zentralen Melderegister eingetragen sind, wird die Stammzahl durch eine mit starker Verschlüsselung gesicherte Ableitung aus ihrer ZMR-Zahl (§ 16 Abs. 1 des Meldegesetzes 1991 – MeldeG, BGBl. Nr. 9/1992) gebildet. Für alle anderen natürlichen Personen ist ihre Ordnungsnummer im Ergänzungsregister (Abs. 4) für die Ableitung der Stammzahl heranzuziehen. Die Benützung der ZMR-Zahl zur Bildung der Stammzahl ist keine Verarbeitung von personenbezogenen Daten des Zentralen Melderegisters im Sinne des § 16a MeldeG.

(3) Für Betroffene, die im Firmenbuch, im Vereinsregister oder im Ergänzungsregister (Abs. 4) eingetragen sind, ist als Stammzahl die Firmenbuchnummer (§ 3 Z 1 des Firmenbuchgesetzes, BGBl. Nr. 10/1991) oder die Vereinsregisterzahl (§ 18 Abs. 3 des Vereinsgesetzes 2002, BGBl. I Nr. 66) oder die im Ergänzungsregister vergebene Ordnungsnummer zu verwenden.

(4) Betroffene, die weder im Melderegister eingetragen sind, noch im Firmenbuch oder im Vereinsregister eingetragen sein müssen, sind auf ihren Antrag oder in den Fällen des § 10 Abs. 2 auf Antrag des Verantwortlichen der Datenverarbeitung im Ergänzungsregister einzutragen. Das Ergänzungsregister wird getrennt nach natürlichen Personen und sonstigen Betroffenen geführt. Voraussetzung für die Eintragung ist bei natürlichen Personen der Nachweis der personenbezogenen Daten, die in der gemäß § 4 Abs. 8 zu erlassenden Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort festgelegt sind, bei sonstigen Betroffenen der Nachweis ihres rechtlichen Bestandes einschließlich ihrer rechtsgültigen Bezeichnung. Im Zuge eines Verfahrens zur Registrierung eines E-ID ist der Nachweis der Identitätsdaten im Sinne des § 1 Abs. 5a MeldeG mit Ausnahme der Melderegisterzahl erforderlich. Zu den sonstigen Betroffenen können Handlungsvollmachten eingetragen werden. Bei welchen Stellen der

apply mutatis mutandis to acting as a representative of natural persons. For represented non-natural persons, the Source PIN Register Authority shall provide the source PIN.

Source PIN

§ 6. (1) The data subject shall be uniquely identified in the eID by his source PIN.

(2) With respect to natural persons who are registered in the Central Register of Residents (CRR), the source identification number shall be derived from that person's registration number in the Central Register of Residents (CRR number) (§ 16 (1) of the Registration Act 1991, Federal Law Gazette No. 9/1992) and secured by using strong cryptography. The source identification number of natural persons, not having to register in the CRR, shall be derived on the basis of their registration number in a Supplementary Register (subparagraph 4). The use of the CRR number in order to generate the source identification number is not to be considered as processing of personal data contained in the CRR for the purposes of § 16a of the Registration Act.

(3) For data subjects entered in the Register of Company Names, the Central Register of Associations or the Supplementary Register the source-PIN shall be the Register of Company Names number (§ 3 No. 1 of the Register of Company Names Act, Federal Law Gazette No. 10/1991) or the Central Register of Associations number (ZVR number) (§ 18 (3) of the Associations Act 2002, Federal Law Gazette I No. 66) or the registration number allocated in the Supplementary Register (subparagraph 4).

(4) Data subjects who are not entered in the Register of Residents and need not be entered in the Register of Company Names nor in the Register of Associations shall be entered in the Supplementary Register upon their application or, in the cases of § 10 (2), upon application by the controller of the data processing system. The Supplementary Register shall be divided into sections for natural persons and for other data subjects. The condition for the registration of natural persons is the proof of the personal data laid down in the regulation of the Federal Minister of Digital and Economic Affairs to be adopted pursuant to § 4 (8) and in the case of other data subjects the proof of their legal existence including their legally valid name. The process of registering an eID requires proof of the identity data pursuant to § 1 (5a) of the Registration Act with exception of the CRR number. It is possible to enter authorities to act for other data subjects. The bodies to which proof of the personal data required for registration in the Supplementary Register may be submitted shall

Nachweis von personenbezogenen Daten für die Eintragung in das Ergänzungsregister erbracht werden kann, ist in der gemäß § 4 Abs. 8 zu erlassenden Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort zu regeln. In dieser Verordnung kann weiters geregelt werden, inwieweit ein Kostenersatz für die Eintragung zu leisten ist.

(5) Elektronische Identifizierungsmittel eines anderen Mitgliedstaats der Europäischen Union, die die Anforderungen des Art. 6 Abs. 1 eIDAS-VO erfüllen, können bei Verantwortlichen des öffentlichen Bereichs wie eine Bürgerkarte für Zwecke der eindeutigen Identifikation im Sinne dieses Bundesgesetzes verwendet werden. Nach Maßgabe der technischen Voraussetzungen hat diese Anerkennung spätestens sechs Monate nach der Veröffentlichung des jeweiligen elektronischen Identifizierungssystems in der Liste gemäß Art. 9 eIDAS-VO zu erfolgen. Bei der Verwendung eines solchen elektronischen Identifizierungsmittels ist für Betroffene, die weder im Melderegister noch im Ergänzungsregister eingetragen sind, ein Eintrag im Ergänzungsregister zu erzeugen. Dafür sind die Personenidentifikationsdaten des verwendeten elektronischen Identifizierungsmittels in das Ergänzungsregister einzutragen. Besteht eine Eintragung für den Betroffenen im Melderegister oder im Ergänzungsregister, sind die Personenidentifikationsdaten des verwendeten elektronischen Identifizierungsmittels in das entsprechende Register einzutragen. Die Stammzahlenregisterbehörde hat auf Antrag des Betroffenen seine Stammzahl direkt der bürgerkartentauglichen Anwendung, bei der die Verfahrenshandlung vorgenommen wird, bereitzustellen. Die Stammzahl darf durch diese nur zur Errechnung von bPK verwendet werden.

(6) Im Stammzahlenregister sind mathematische Verfahren zur Bildung der Stammzahl bei natürlichen Personen zu verwenden, die die ZMR-Zahl oder die Ordnungsnummer des Ergänzungsregisters stark verschlüsseln. Diese Verfahren sind durch die Stammzahlenregisterbehörde festzulegen und – mit Ausnahme der verwendeten kryptographischen Schlüssel – im Internet zu veröffentlichen.

Stammzahlenregisterbehörde

§ 7. (1) Stammzahlenregisterbehörde ist der Bundesminister für Digitalisierung und Wirtschaftsstandort.

(2) Die Stammzahlenregisterbehörde kann sich bei der Führung des Ergänzungsregisters sowie bei der Errechnung von Stammzahlen und bei der Durchführung der in den §§ 4, 4b, 5, 9, 10, 14, 14a und 15 geregelten Verfahren des

be specified in the regulation of the Federal Minister of Digital and Economic Affairs to be adopted pursuant to § 4(8). Moreover, that regulation shall govern to which extent the costs caused by registration must be reimbursed.

(5) Electronic identification means of another Member State of the European Union that meet the requirements of Art. 6(1) of the eIDAS Regulation can be used for public-sector controllers like a citizen card for the purposes of unique identification as defined in this Federal Act. In accordance with the technical prerequisites, such electronic identification means must be recognised no later than six months after publication of the relevant electronic identification scheme in the list pursuant to Art. 9 of the eIDAS Regulation. When such electronic identification means are used, an entry in the Supplementary Register must be created for data subjects who have neither been entered in the Central Register of Residents nor in the Supplementary Register. For this purpose, the person identification data of the electronic identification means used must be entered in the Supplementary Register. If an entry for the data subject exists in the Central Register of Residents or in the Supplementary Register, the person identification data of the electronic identification means used must be entered in the relevant register. The Source PIN Register Authority shall, upon application of the data subject, provide the source PIN of the data subject directly to the citizen card enabled application where the official procedure is carried out. The source PIN may be used by the Source PIN Register Authority only to generate sector-specific personal identifiers.

(6) For the generation of source identification numbers for natural persons the source-PIN Register Authority has to use mathematical algorithms which apply strong cryptography to the central popular register number or the indenture number of the Supplementary Register. These algorithms shall be determined by the source-PIN Register Authority and – with the exception of the cryptographic key used – published on the Internet.

Source PIN Register Authority

§ 7. (1) The Federal Minister of Digital and Economic Affairs is the Source PIN Register Authority.

(2) In maintaining the Supplementary Register, generating source identification numbers and conducting the procedures governed by § 4, § 4b, § 5, § 9,§ 10, § 14, § 14a and § 15, the Source PIN Register Authority may have recourse

Bundesministeriums für Inneres als Auftragsverarbeiter, soweit natürliche Personen Betroffene sind, und des Bundesministeriums für Finanzen oder der Bundesanstalt Statistik Österreich hinsichtlich aller anderen Betroffenen bedienen. Die näheren Regelungen über die sich daraus ergebende Aufgabenverteilung zwischen der Stammzahlenregisterbehörde und dem Bundesministerium für Inneres, dem Bundesministerium für Finanzen oder der Bundesanstalt Statistik Österreich als Auftragsverarbeiter werden durch Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort im Einvernehmen mit dem Bundesminister für Inneres, dem Bundesminister für Finanzen oder dem Bundeskanzler geregelt. Abweichend davon kann sich die Stammzahlenregisterbehörde für diese Zwecke auch anderer oder weiterer Auftragsverarbeiter bedienen. Die Stammzahlenregisterbehörde hat stichprobenartig die ordnungsgemäße Erfüllung der Aufgaben der Auftragsverarbeiter zu prüfen.

Eindeutige Identifikation in Datenverarbeitungen

§ 8. In den Datenverarbeitungen von Verantwortlichen des öffentlichen Bereichs darf eine im Rahmen des Konzepts des E-ID erfolgende eindeutige Identifikation von Betroffenen im Hinblick auf natürliche Personen nur in Form des bPK (§ 9) dargestellt werden. Für Betroffene, die keine natürlichen Personen sind, darf zur eindeutigen Identifikation die Stammzahl gespeichert werden.

Bereichsspezifisches Personenkennzeichen (bPK)

§ 9. (1) Das bPK wird durch eine Ableitung aus der Stammzahl der betroffenen natürlichen Person gebildet. Die Identifikationsfunktion dieser Ableitung ist auf jenen staatlichen Tätigkeitsbereich beschränkt, dem die Datenverarbeitung zuzurechnen ist, in der das bPK verarbeitet werden soll. Die Zurechnung einer Datenverarbeitung zu einem bestimmten staatlichen Tätigkeitsbereich ergibt sich aus ihrer Registrierung bei der Stammzahlenregisterbehörde.

(2) Die Abgrenzung der staatlichen Tätigkeitsbereiche ist für Zwecke der Bildung von bPK so vorzunehmen, dass zusammengehörige Lebenssachverhalte in ein- und demselben Bereich zusammengefasst werden und miteinander unvereinbare Datenverarbeitungen innerhalb desselben Bereichs nicht vorgesehen sind. Die Bezeichnung und Abgrenzung dieser Bereiche wird durch Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort festgelegt; vor Erlassung oder Änderung dieser Verordnung sind die Länder und die Gemeinden, letztere vertreten durch den Österreichischen Gemeindebund und den Österreichischen Städtebund, anzuhören.

to the Federal Ministry of the Interior as a processor, insofar as natural persons are concerned, and to the Federal Ministry of Finance or Statistics Austria, insofar as all other data subjects are concerned. The detailed provisions governing the distribution of functions between the Source PIN Register Authority and the Federal Ministry of the Interior, the Federal Ministry of Finance or Statistics Austria as a processor shall be laid down in a regulation of the Federal Minister of Digital and Economic Affairs with the consent of the Federal Minister of the Interior, the Federal Minister of Finance or the Federal Chancellor. By way of derogation from the above, the Source PIN Register Authority can also use other or further processors for these purposes. The Source PIN Register Authority shall randomly check that the tasks of the processors are completed correctly.

Unique identification in data processing systems

§ 8. In the data processing systems of public-sector controllers, the unique identification of natural persons within the framework of the eID scheme may be represented only in the form of a sector-specific personal identifier (§ 9). With respect to data subjects who are not natural persons, the source identification number may be stored for the purpose of unique identification.

Sector-specific personal identifiers

§ 9. (1) The sector-specific personal identifier is derived from the source identification number of a data subject who is a natural person. The use of that derived identifier for identification purposes shall be limited to that sector of State activity to which the data processing system in which the sector-specific personal identifier is to be processed is to be allocated. A data processing system is allocated to a specific sector of State activity on the basis of its registration with the Source PIN Register Authority.

(2) For the purpose of generating sector-specific personal identifiers, sectors of State activity are to be delimited in such a way as to ensure that associated situations fall within the same sector and to prevent incompatible data processing systems within the same sector. The description and delimitation of those areas shall be determined in a regulation of the Federal Minister of Digital and Economic Affairs. The provinces and the municipalities, the latter represented by the Austrian Association of Municipalities and the Austrian Association of Cities and Towns, shall be consulted prior to adoption of that regulation.

(3) Die zur Bildung des bPK eingesetzten mathematischen Verfahren (Hash-Verfahren über die Stammzahl und die Bereichskennung) werden von der Stammzahlenregisterbehörde festgelegt und – mit Ausnahme der verwendeten kryptographischen Schlüssel – im Internet veröffentlicht.

Erzeugung und Anforderung von bPK und Stammzahlen nicht-natürlicher Personen

§ 10. (1) Bei Verwendung des E-ID werden bPK eines Betroffenen in elektronischen Verfahren erzeugt, für die der Verantwortliche des öffentlichen Bereichs eine E-ID-taugliche Umgebung eingerichtet hat. Dafür muss eine Datenverarbeitung mit ihrer Zuordnung zu einem staatlichen Bereich bei der Stammzahlenregisterbehörde registriert sein. In Bereichen, in denen der Verantwortliche des öffentlichen Bereichs nicht zur Vollziehung berufen ist, dürfen bPK nur verschlüsselt (§ 13 Abs. 2) gespeichert werden.

(2) Die Erzeugung von bPK ohne Einsatz des E-ID ist nur der Stammzahlenregisterbehörde erlaubt und nur zulässig, wenn eine eindeutige Identifikation mit Hilfe des bPK im Rahmen von Datenverarbeitungen von Verantwortlichen des öffentlichen Bereichs notwendig ist, weil personenbezogene Daten in einer der DSGVO und dem DSG entsprechenden Art und Weise verarbeitet werden sollen. Solche Fälle sind insbesondere Amtshilfe, Datenermittlung im Auftrag des Betroffenen oder das Einschreiten eines Vertreters gemäß § 5. Aus denselben Gründen ist bei nicht-natürlichen Personen die Stammzahl zur Verfügung zu stellen. Bei der Anforderung von bPK aus einem Bereich, in dem der Verantwortliche des öffentlichen Bereichs nicht zur Vollziehung berufen ist, oder von bPK für die Verarbeitung im privaten Bereich dürfen bPK nur verschlüsselt (§ 13 Abs. 2) zur Verfügung gestellt werden.

(3) In der gemäß § 4 Abs. 8 zu erlassenden Verordnung ist auch der Kostenersatz für die nach Abs. 2 im Zusammenhang mit berufsmäßiger Parteienvertretung erfolgte Bereitstellung von bPK zu regeln.

Offenlegung von bPK in Mitteilungen

§ 11. In Mitteilungen an den Betroffenen oder an Dritte sind bPK nicht anzuführen. Die Erleichterung der Zuordnung solcher Mitteilungen zu Aufzeichnungen beim Verantwortlichen über denselben Gegenstand ist auf andere Weise, wie etwa durch Anführung einer Geschäftszahl, zu bewerkstelligen.

(3) The mathematical algorithms applied to generate the sector-specific personal-identifier (hash function using the source identification number und the sector code) shall be determined by the source-PIN Register Authority and – with the exception of any cryptographic keys used – published on the Internet.

Generation and requirements of sector-specific personal identifiers and source identification numbers of non-natural persons

§ 10. (1) By using an eID, a data subject's sector-specific personal identifier is generated in electronic procedures for which a public-sector controller has created an environment in which the eID may be used. For that purpose, a data processing system, together with its allocation to a sector of State activity, must be registered with the Source PIN Register Authority. In sectors in which the public-sector controller has not been entrusted with implementation duties, only encrypted (§ 13 (2)) sector-specific personal identifiers may be stored.

(2) The generation of sector-specific personal identifiers without the use of an eID is only allowed for the Source PIN Register Authority and is only permissible when the unique identification on the basis of the sector-specific personal identifier in data processing systems of public-sector controllers is necessary because personal data are to be processed in conformity with the GDPR and the Data Protection Act. Such cases include, in particular, administrative cooperation, data acquisition at the request of the data subject or a submission to an authority by a representative pursuant to § 5. For the same reasons, the source PIN shall be made available for non-natural persons. In the event of a request for sector-specific personal identifiers from a sector in which the public-sector controller has not been entrusted with implementation duties or for sector-specific personal identifiers for processing in the private sector, only sector-specific personal identifiers which have been encrypted (§ 13 (2)) may be made available.

(3) The reimbursement of the costs of the supply of sector-specific personal identifiers in connection with professional representation pursuant to subparagraph 2 shall also be governed by the regulation to be adopted pursuant to § 4(8).

Disclosure of sector-specific personal identifiers in communications

§ 11. Sector-specific personal-identifiers shall not be stated in communications to data subjects or to third parties. The matching of such communications to records of the controller concerning the same subject matter shall be facilitated by other means, such as a reference number.

Schutz der Stammzahl natürlicher Personen

§ 12. (1) Die Vertraulichkeit von Stammzahlen natürlicher Personen unterliegt besonderem Schutz durch folgende Vorkehrungen im Konzept des E-ID:

1. Eine dauerhafte Speicherung der Stammzahl natürlicher Personen darf nur in verschlüsselter Form erfolgen.
2. Die Verarbeitung der Stammzahl natürlicher Personen im Errechnungsvorgang für das bPK darf zu keiner Speicherung der Stammzahl außerhalb des Errechnungsvorgangs führen. Der Vorgang der Errechnung darf nur bei der Stammzahlenregisterbehörde oder bei der in ihrem Auftrag tätigen Behörde, die in der gemäß § 4 Abs. 8 zu erlassenden Verordnung näher zu bezeichnen sind, durchgeführt werden.

(2) Die Verarbeitung der Stammzahl zur Ermittlung eines bPK darf nur erfolgen:

1. unter Mitwirkung des E-ID-Inhabers nach den Bestimmungen der §§ 4 Abs. 5, 14 Abs. 3 und 14a Abs. 2, oder
2. ohne Mitwirkung des Betroffenen durch die Stammzahlenregisterbehörde nach den näheren Bestimmungen der §§ 10, 13 Abs. 2 und 15.

Weitere Garantien zum Schutz von bPK

§ 13. (1) bPK sind durch nicht-umkehrbare Ableitungen aus der Stammzahl zu bilden. Dies gilt im Interesse der Nachvollziehbarkeit staatlichen Handelns nicht für bPK, die ausschließlich im Zusammenhang mit der Tätigkeit einer Person als Organwalter verarbeitet werden.

(2) Ist es zum Zweck der eindeutigen Identifikation eines Betroffenen gemäß § 10 Abs. 2 zulässig, von der Stammzahlenregisterbehörde ein bPK anzufordern, ist dieses, sofern es sich um ein bPK aus einem Bereich handelt, in dem der Anfordernde nicht zur Vollziehung berufen ist oder es sich um ein bPK für die Verwendung im privaten Bereich handelt, von der Stammzahlenregisterbehörde nur verschlüsselt zur Verfügung zu stellen. Die Verschlüsselung ist so zu gestalten, dass

Protection of the source PIN of natural persons

§ 12. (1) The confidentiality of source identification numbers of natural persons shall be subject to special protection by way of the following measures of the eID scheme:

1. The source identification number of natural persons may be permanently stored only in encrypted form.
2. The processing of the source identification number of natural persons in order to generate the sector-specific personal identifier must not give rise to any storage of the source identification number outside of the generation process. The process of generating sector-specific personal identifiers may only be carried out at the Source PIN Register Authority or an authority acting on its behalf, which must be specified in the regulation to be adopted pursuant to § 4(8).

(2) The source identification number may be processed to generate a sector-specific personal identifier only:

1. with the cooperation of the eID holder in accordance with the provisions of § 4(5), § 14(3) and § 14a(2), or
2. without the cooperation of the data subject by the source-PIN Register Authority in accordance with the detailed provisions of § 10, § 13(2) and § 15.

Further guarantees for the protection of sector-specific personal identifiers

§ 13. (1) Sector-specific personal identifiers shall be generated by irreversible derivations from the source identification number. In the interests of the transparency of State activity, this shall not apply to sector-specific personal identifiers which are processed exclusively in connection with the activity of a person as an official representing a public authority.

(2) Where it is permissible under § 10(2) to request from the source-PIN Register Authority a sector-specific personal-identifier for the purpose of the unique identification of a data subject, the source-PIN Register Authority may, insofar as a sector-specific personal-identifier for a sector in which the requester has not been entrusted with implementation duties is concerned or it is a sector-specific personal-identifier for a private sector, provide the sector-specific personal-identifier in encrypted form only. The form of that encryption must be such as to ensure that:

1. nur derjenige entschlüsseln kann, in dessen Datenverarbeitung das bPK in entschlüsselter Form zulässigerweise verarbeitet werden darf (Abs. 3), und

2. durch Einbeziehung von zusätzlichen, dem Anfordernden nicht bekannten variablen Angaben in die Verschlüsselungsbasis das bPK auch in verschlüsselter Form keinen personenbezogenen Hinweis liefert.

(3) bPK dürfen unverschlüsselt in einer Datenverarbeitung nur dann gespeichert werden, wenn zur Bildung des bPK die Kennung jenes Bereichs verwendet wurde, der die Datenverarbeitung in Übereinstimmung mit der gemäß § 9 Abs. 2 erlassenen Verordnung zuzurechnen ist.

3. Abschnitt

Verwendung der Funktion E-ID im privaten Bereich oder bei Anwendungen im Ausland

Erzeugung von bPK für die Verwendung des E-ID im privaten Bereich

§ 14. (1) Für die eindeutige Identifikation von natürlichen Personen im elektronischen Verkehr mit einem Verantwortlichen des privaten Bereichs (§ 26 Abs. 4 DSG) kann durch Einsatz des E-ID ein bPK gebildet werden, wobei anstelle der Bereichskennung die Stammzahl des Verantwortlichen des privaten Bereichs tritt. Voraussetzung hiefür ist, dass der Verantwortliche des privaten Bereichs eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet hat, in der seine Stammzahl als Bereichskennung im Errechnungsvorgang für das bPK zur Verfügung gestellt wird.

(2) Verantwortliche des privaten Bereichs dürfen nur solche bPK speichern und benützen, die mit Hilfe ihrer eigenen Stammzahl als Bereichskennung gebildet wurden.

(3) Bei der Verwendung des E-ID im elektronischen Verkehr gemäß Abs. 1 ist auf Basis der vom qualifizierten VDA zur Verfügung gestellten verschlüsselten Stammzahl durch die Stammzahlenregisterbehörde oder die in ihrem Auftrag tätige Behörde eine Personenbindung (§ 4 Abs. 2), die ein bPK zum E-ID-Inhaber enthält, zu erstellen, und an die betreffende Datenverarbeitung zu übermitteln. Mit Einwilligung des E-ID-Inhabers können in die Personenbindung die vom

1. only the controller in whose data processing system it is permissible to process the sector-specific personal identifier in decrypted form is able to decrypt it (subparagraph 3), and

2. as a result of the inclusion in the basis for encryption of additional variable data of which the requesting party has no knowledge, the sector-specific personal-identifier cannot, even in encrypted form, supply any information on the data subject.

(3) Sector-specific personal identifiers may be stored in a data processing system in unencrypted form only where, in order to generate the sector-specific personal identifier, use was made of the code for the sector to which the data processing system is to be allocated in accordance with the regulation to be adopted pursuant to § 9(2).

Part III

Use of the eID function in the private sector or abroad

Generation of sector-specific personal identifiers for use of the eID in the private sector

§ 14. (1) For the unique identification of natural persons in electronic communications with a private-sector controller (§ 26 (4) of the Data Protection Act), a sector-specific personal identifier may be derived using the eID, wherein the source PIN of the private-sector controller replaces the sector code. This shall be subject to the condition that the private-sector controller has set up a technical environment in which the eID can be used and in which the controller's source-PIN is made available as the sector code for the generation of the sector-specific personal identifier.

(2) Private-sector controllers may store and use only such sector-specific personal identifiers that have been generated using their own source identification number as sector code.

(3) When the eID is used in electronic communications pursuant to subparagraph 1, the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (§ 4(2)) containing a sector-specific personal identifier relating to the eID holder on the basis of the encrypted source PIN provided by the qualified TSP and send it to the relevant data processing system. With the consent of the eID holder, the personal data to be provided by the qualified

qualifizierten VDA zur Verfügung zu stellenden personenbezogenen Daten, das sind Vorname, Familienname oder Geburtsdatum, sowie nach Maßgabe der technischen Möglichkeiten weitere Merkmale zu diesem aus für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen Bereichs eingefügt werden. § 4 Abs. 6 ist sinngemäß anzuwenden.

E-ID-taugliche Anwendungen im Ausland

§ 14a. (1) Für E-ID-taugliche Anwendungen im Ausland ist § 14 Abs. 1 mit der Maßgabe anzuwenden, dass anstelle der Bereichskennung ein staatenspezifisches Kennzeichen oder bei Anwendungen internationaler Organisationen ein organisationsspezifisches Kennzeichen zu verwenden ist.

(2) Bei der Verwendung des E-ID im elektronischen Verkehr gemäß Abs. 1 ist durch die Stammzahlenregisterbehörde oder die in ihrem Auftrag tätige Behörde eine Personenbindung (§ 4 Abs. 2), die ein bPK, Vorname, Familienname und Geburtsdatum zum E-ID-Inhaber enthält, zu erstellen, und an die betreffende Datenverarbeitung zu übermitteln. Zu diesem Zweck hat der qualifizierte VDA die verschlüsselte Stammzahl, Vorname, Familienname und Geburtsdatum der Stammzahlenregisterbehörde zur Verfügung zu stellen. Nach Maßgabe der technischen Möglichkeiten können mit Einwilligung des E-ID-Inhabers in die Personenbindung weitere Merkmale zu diesem aus für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen Bereichs eingefügt werden.

Garantien zum Schutz der Stammzahl und der bPK bei der Verarbeitung im privaten Bereich

§ 15. (1) Die Erzeugung eines bPK für die Verarbeitung im privaten Bereich ist ohne Mitwirkung des Betroffenen und ohne Einsatz des E-ID zulässig, wenn eine eindeutige Identifikation mit Hilfe des bPK im Rahmen von Datenverarbeitungen von Verantwortlichen des privaten Bereichs notwendig ist, weil

1. diese Verantwortlichen aufgrund gesetzlicher Vorschriften die Identität ihrer Kunden festzuhalten haben oder ihren Kunden eine dem § 14 Abs. 1 zweiter Satz entsprechende technische Umgebung zur Verfügung stellen und
2. personenbezogene Daten in einer der DSGVO und dem DSG entsprechenden Art und Weise verarbeitet werden sollen.

Sofern ein Verantwortlicher des privaten Bereichs personenbezogene Daten an einen anderen Verantwortlichen zu übermitteln hat, kann dieser wie ein

TSP, i.e. the first name, family name or date of birth, and, in accordance with the technical possibilities, further data of the eID holder taken from registers of public-sector controllers which the Source PIN Register Authority can access can be included in the identity link. § 4 (6) shall apply mutatis mutandis.

eID-compatible applications abroad

§ 14a. (1) For eID-compatible applications abroad § 14 (1) shall be applied subject to the proviso that the sector code replaces a specific state code or for applications of international organizations a specific organizational code.

(2) When the eID is used in electronic communications pursuant to subparagraph 1, the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (§ 4 (2)) containing a sector-specific personal identifier, the first name, family name and date of birth of the eID holder and send it to the relevant data processing system. For this purpose, the qualified TSP shall provide to the Source PIN Register Authority the encrypted source PIN, the first name, family name and date of birth. In accordance with the technical possibilities, further data of the eID holder taken from registers of public-sector controllers which the Source PIN Register Authority can access can be included in the identity link with the consent of the eID holder.

Guarantees for the protection of source identification numbers and sector-specific personal identifiers when processed in the private sector

§ 15. (1) The generation of a sector-specific personal identifier for processing in the private sector requires no collaboration of the data subject and no use of the eID if a unique identification by means of a sector-specific personal identifier in data processing systems of private-sector controllers is necessary because

1. these controller have to establish the unique identity of their customers because of statutory provisions or provide a technical environment corresponding to § 14 (1) second sentence to their clients and
2. personal data will be processed and transmitted in conformity with the GDPR and the Data Protection Act.

As far as a private-sector controller must transmit personal data to another controller, this controller can request encrypted sector-specific personal identifiers (§ 13 (2)) like a public-sector controller.

Verantwortlicher des öffentlichen Bereichs verschlüsselte bPK (§ 13 Abs. 2) anfordern.

(2) Der Bundesminister für Inneres ist ermächtigt, einen Kostenersatz für den für die Erzeugung der bPK und der verschlüsselten bPK gemäß Abs. 1 anfallenden Aufwand mit Verordnung festzulegen.

(2) The Federal Minister of the Interior is authorized to determine by ordinance a reimbursement of costs for the investment the generation of sector-specific personal identifiers and the encrypted sector-specific personal identifiers corresponding to subparagraph 1.

4. Abschnitt
Elektronischer Datennachweis

für personenbezogene Daten über selbständige wirtschaftliche Tätigkeiten

§ 16. (1) Der elektronische Nachweis über die Art einer selbständigen Erwerbstätigkeit und über das Vorliegen der hiefür notwendigen Berufsberechtigungen kann durch Inanspruchnahme des Dokumentationsregisters nach § 114 Abs. 2 BAO geführt werden.

(2) Soweit der Nachweis der in Abs. 1 bezeichneten personenbezogenen Daten in Verfahren vor einem Verantwortlichen des öffentlichen Bereichs notwendig ist, kann er vom Betroffenen selbst durch Vorlage der vom Dokumentationsregister elektronisch signierten oder besiegelten Auskunft erbracht oder auf Ersuchen des Betroffenen durch den Verantwortlichen im Wege der elektronischen Einsicht in das Register beschafft werden. Die amtswegige Beschaffung des Nachweises ist bei Vorliegen der gesetzlichen Voraussetzungen für diese Datenermittlung zulässig.

für personenbezogene Daten aus Registern

§ 17. (1) Soweit die Richtigkeit der im Zentralen Melderegister gespeicherten personenbezogenen Daten zum Personenstand und zur Staatszugehörigkeit von den Meldebehörden durch Einsicht in die entsprechenden Dokumente (Standarddokumente) geprüft wurde, haben sie dies dem Zentralen Melderegister mitzuteilen, worauf die erfolgte Prüfung im Zentralen Melderegister in geeigneter Weise elektronisch lesbar anzumerken ist. Diese Anmerkung kann vom Betroffenen auch außerhalb eines Meldevorgangs verlangt werden, wenn er der Meldebehörde die Richtigkeit eines Meldedatums durch Vorlage der entsprechenden Dokumente nachweist.

(2) Ist von Behörden die Richtigkeit von personenbezogenen Daten zu beurteilen, die in einem elektronischen Register eines Verantwortlichen des öffentlichen Bereichs enthalten sind, haben sie nach Maßgabe der technischen

Part IV
Electronic validation of data

for personal data on economic activities as a self-employed person

§ 16. (1) Electronic validation of the nature of a self-employed activity and of fulfilment of the professional requirements for pursuit of that activity may be obtained from the Documentation Register under § 114(2) of the Federal Fiscal Code.

(2) Where validation of the personal data referred to in subparagraph 1 is required in procedures involving a public-sector controller, the data subject may himself supply it by submitting a copy signed or sealed electronically by the Documentation Register or, at the request of the data subject, the controller may acquire it by way of electronic access to the Documentation Register. It shall be permissible to obtain validation through official channels where the statutory requirements for such data acquisition are satisfied.

for personal data from registers

§ 17. (1) Where the accuracy of the personal data stored in the Central Register of Residents with regard to personal status and nationality has been verified by the local registration authorities by way of inspection of the appropriate documents (standard documents), those authorities must inform the Central Register of Residents thereof and the fact that the data has been verified shall be noted in the Central Register of Residents in a suitable, electronically legible form. The data subject may request that such information be entered even outside a procedure for registration of residence if he provides the registration authority with proof of the accuracy of the registration data by submitting the appropriate documents.

(2) If authorities must determine the accuracy of personal data contained in an electronic register of a public-sector controller they themselves shall with the proviso of technical possibilities undertake the acquisition of the data via electronic

Möglichkeiten, wenn die Einwilligung des Betroffenen zur Datenermittlung oder eine gesetzliche Ermächtigung zur amtswegigen Datenermittlung vorliegt, die Datenermittlung im Wege des Datenfernverkehrs, sofern dies erforderlich ist, selbst durchzuführen. Die Behörde hat den Betroffenen auf die Möglichkeit der Einwilligung zur Datenermittlung hinzuweisen. Die Datenermittlung ersetzt die Vorlage eines Nachweises der personenbezogenen Daten durch die Partei oder den Beteiligten. Elektronische Anfragen an das Zentrale Melderegister sind im Wege des § 16a Abs. 4 MeldeG zu behandeln.

(3) Die Betroffenen können von der elektronischen Verfügbarkeit geprüfter Meldedaten Gebrauch machen, indem sie

1. in Verfahren, in welchen die Vorlage von Standarddokumenten im Sinne des Abs. 1 erforderlich ist, in die Beschaffung der benötigten personenbezogenen Daten aus dem Zentralen Melderegister einwilligen oder
2. eine mit Amtssignatur (§ 19) elektronisch signierte oder besiegelte Meldebestätigung des Zentralen Melderegisters anfordern, in der die Tatsache der geprüften Richtigkeit bei den einzelnen Meldedaten angemerkt ist.

über personenbezogene Daten aus elektronischen Registern eines Verantwortlichen des öffentlichen Bereichs

§ 18. (1) Personenbezogene Daten, die gemäß § 4b Z 1 bis 5 und 8 oder in einem für die Stammzahlenregisterbehörde zugänglichen elektronischen Register eines Verantwortlichen des öffentlichen Bereichs enthalten sind, sind bei der Verwendung der Funktion E-ID nach Maßgabe der technischen Möglichkeiten

1. dem E-ID-Inhaber selbst, oder
2. Dritten im Auftrag des E-ID-Inhabers, sofern ihnen die Nutzung des E-ID-Systems eröffnet und noch nicht unterbunden wurde

zur Verfügung zu stellen.

(2) Der Bundesminister für Inneres ist ermächtigt, Dritten nach Abs. 1 Z 2 die Nutzung des E-ID-Systems zu eröffnen. Die Nutzung ist nicht zu eröffnen oder zu unterbinden, wenn Anhaltspunkte dafür bestehen, dass Dritte die ihnen zur Verfügung gestellten personenbezogenen Daten nicht gemäß dem Grundsatz nach Treu und Glauben und auf rechtmäßige Weise verarbeitet haben.

(3) Der Bundesminister für Inneres hat im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort nähere Bestimmungen

communications to the extent this is necessary provided that the data subject has consented to or that such an acquisition through official channels is authorised by statute. The authorities shall advise the data subject of the possibility of consenting to the data acquisition. Data acquisition shall replace the presentation of proof of the personal data by the parties or persons involved. Electronic requests to the Central Register of Residents shall be treated in accordance with § 16a (4) of the Registration Act 1991.

(3) The data subject may make use of the electronic availability of verified registration data by:

1. consenting to the acquisition of the personal data required from the Central Register of Residents in procedures in which it is necessary to submit standard documents within the meaning of subparagraph 1; or
2. requesting from the Central Register of Residents a confirmation of registration which has been signed or sealed electronically with an official signature (§ 19) and which states that the accuracy of the individual registration data has been verified.

regarding personal data from electronic registers of a public-sector controller

§ 18. (1) When the eID function is used, personal data contained pursuant to § 4b Nos. 1 to 5 and 8 or in an electronic register of a public-sector controller which the Source PIN Register Authority can access must be provided, in accordance with the technical possibilities,

1. to the eID holder, or
2. to third parties on behalf of the eID holder, provided they were allowed to use the eID system and have not been prohibited from using it.

(2) The Federal Minister of the Interior is authorised to allow third parties as referred to in subparagraph 1 No. 2 to use the eID system. They must not be allowed to use it or must be prohibited from using it if there is indication that such third parties have not processed the personal data provided to them fairly and lawfully.

(3) The Federal Minister of the Interior, with the consent of the Federal Minister of Digital and Economic Affairs, shall specify, by regulation, detailed

über die Vorgangsweise gemäß Abs. 1 und 2 durch Verordnung festzulegen. Dabei ist jedenfalls sicherzustellen, dass die Protokollierung der Datenübermittlung aus dem E-ID-System an Dritte im Auftrag des E-ID-Inhabers nur diesem zugänglich ist.

5. Abschnitt
Besonderheiten elektronischer Aktenführung

Amtssignatur

§ 19. (1) Die Amtssignatur ist eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel, deren Besonderheit durch ein entsprechendes Attribut im Signaturzertifikat oder Zertifikat für elektronische Siegel ausgewiesen wird.

(2) Die Amtssignatur dient der erleichterten Erkennbarkeit der Herkunft eines Dokuments von einem Verantwortlichen des öffentlichen Bereichs. Sie darf daher ausschließlich von diesem Verantwortlichen des öffentlichen Bereichs unter den näheren Bedingungen des Abs. 3 bei der elektronischen Unterzeichnung und bei der Ausfertigung der von ihm erzeugten Dokumente verwendet werden.

(3) Die Amtssignatur ist im Dokument durch eine Bildmarke, die der Verantwortliche des öffentlichen Bereichs im Internet als die seine gesichert veröffentlicht hat, sowie durch einen Hinweis im Dokument, dass dieses amtssigniert wurde, darzustellen. Die Informationen zur Prüfung der elektronischen Signatur oder des elektronischen Siegels sind vom Verantwortlichen des öffentlichen Bereichs bereitzustellen.

Beweiskraft von Ausdrucken

§ 20. Ein auf Papier ausgedrucktes elektronisches Dokument einer Behörde hat die Beweiskraft einer öffentlichen Urkunde (§ 292 der Zivilprozessordnung – ZPO, RGBl. Nr. 113/1895), wenn das elektronische Dokument mit einer Amtssignatur versehen wurde. Die Amtssignatur muss durch Rückführung des Dokuments aus der ausgedruckten in die elektronische Form prüfbar oder das Dokument muss durch andere Vorkehrungen der Behörde verifizierbar sein. Das Dokument hat einen Hinweis auf die Fundstelle im Internet, wo das Verfahren der Rückführung des Ausdrucks in das elektronische Dokument und die anwendbaren Prüfmechanismen enthalten sind, oder einen Hinweis auf das Verfahren der Verifizierung zu enthalten.

provisions on the procedure pursuant to subparagraphs 1 and 2. In that regard it must be ensured that solely the eID holder has access to records relating to the transfer of data from the eID system to third parties effected on behalf of the eID holder.

Part V
Special characteristics of keeping electronic records

Official signature

§ 19. (1) An official signature is an advanced electronic signature or an advanced electronic seal, which is indicated as being special by an appropriate attribute in the signature certificate or certificate for electronic seals.

(2) An official signature serves to facilitate recognition of the fact that a document originates from a public-sector controller. It may therefore only be used by this public-sector controller in accordance with the detailed conditions laid down in subparagraph 3, when signing electronically or drawing up the documents issued by the controller.

(3) The official signature in views of electronic documents shall be displayed by means of an image which the public-sector controller has published on the Internet in secure form as its own and a reference within the document confirming that it has been officially signed. The information needed for the validation of the electronic signature or the electronic seal has to be provided by the public-sector controller.

Probative value of printouts

§ 20. An electronic document of an authority printed out on to paper is assumed to be authentic (§ 292 of the Code of Civil Procedure, Imperial Law Gazette No. 113/1895) if signed with an official signature. The official signature has to allow verification by reconverting the printout of the document into its electronic form or the document must be verifiable by other means provided by the authority. The document shall include a reference to the source on the Internet, containing the procedure for reconverting the printout into the electronic form and the applicable verification mechanisms, or a reference to another verification process.

Vorlage elektronischer Akten

§ 21. (1) Soweit von einer Behörde Akten an eine andere Behörde vorgelegt werden müssen, und diese Akten elektronisch erzeugt und elektronisch genehmigt wurden, bezieht sich die Vorlagepflicht auf dieses elektronische Original. Dies gilt insbesondere für Akten aus einem durchgehend elektronisch geführten Aktenbearbeitungs- und -verwaltungssystem. Die Vorlage muss in einem Standardformat erfolgen.

(2) Als Standardformate gelten jene elektronischen Formate, die die Lesbarkeit eines Dokuments auch für Dritte während der voraussichtlichen Aufbewahrungsdauer nach dem Stand der Technik jeweils bestmöglich gewährleisten.

(3) Hat die Behörde, der der elektronische Akt vorzulegen ist, einen elektronischen Zustelldienst mit der Entgegennahme von Sendungen für die Behörde betraut, kann die Aktenvorlage, insbesondere wenn sie nachweisbar sein soll, auch über diesen Zustelldienst erfolgen. Die Bestimmungen des 3. Abschnitts des Zustellgesetzes gelten diesfalls sinngemäß mit der Maßgabe, dass die Vorlage mit dem auf die elektronische Absendung der Verständigung von der Bereitstellung folgenden Tag bewirkt wird.

Submission of electronic records

§ 21. (1) Where an authority is required to submit records to another authority and those records were generated and approved electronically, the duty to submit relates to the electronic original. This applies, in particular, to records which are kept in an entirely electronically operated file processing and management system. The document must be submitted in a standard format.

(2) Standard formats are such electronic formats which, using the latest available technology, guarantee the best legibility of a document possible, from the point of view of third parties also, during the period for which it is envisaged that the document is to be kept.

(3) Where the authority to which the electronic record is to be submitted has authorised an electronic delivery service to receive correspondence addressed to it, the record may also be submitted to that agent, in particular, where proof of submission is required. In such cases, the provisions in Part 3 of the Service of Documents Act shall apply mutatis mutandis, subject to the condition that the document is to be considered as submitted on the day following the electronic dispatch of notification that the document is available for retrieval from the server of the delivery service.

5a. Abschnitt
Haftungsbestimmungen

Haftung

§ 21a. (1) Umfang und Ausmaß des nach Art. 11 der eIDAS-VO zu ersetzenden Schadens, sowie allfällige Rückgriffsrechte gegenüber anderen Personen, richten sich nach den auf den Schadensfall sonst anwendbaren Bestimmungen.

(2) Ersatzansprüche gegenüber anderen Personen oder aus einem anderen Rechtsgrund bleiben unberührt.

Part Va
Liability provisions

Liability

§ 21a. (1) The scope and extent of the damage to be compensated pursuant to Art. 11 of the eIDAS Regulation and any rights of recovery from other persons depend on the other provisions applicable to the damage.

(2) Any claim for damages towards other persons or on any other legal ground shall remain unaffected.

6. Abschnitt
Strafbestimmungen

Unzulässige Verarbeitung von Stammzahlen oder bPK oder unzulässige Verwendung von Amtssignaturen

§ 22. (1) Sofern die Tat nicht nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die von der Bezirksverwaltungsbehörde mit Geldstrafe bis zu 20 000 Euro zu ahnden ist, wer

1. sich die Stammzahl einer natürlichen Person oder deren bPK entgegen den Bestimmungen des 2. oder 3. Abschnitts verschafft, um sie für die rechtswidrige Ermittlung personenbezogener Daten des Betroffenen einzusetzen, oder
2. ein bPK eines anderen Verantwortlichen des privaten Bereichs unbefugt speichert oder benützt oder
3. anderen Verantwortlichen des privaten Bereichs die mit der eigenen Stammzahl gebildeten bPK in einer unzulässigen Weise zur Verfügung stellt oder
4. als Verantwortlicher des privaten Bereichs ein bPK dazu benützt, um Dritten personenbezogene Daten über einen gemeldeten Wohnsitz des Betroffenen zu verschaffen oder
5. eine Amtssignatur entgegen § 19 Abs. 2 verwendet oder ihre Verwendung vortäuscht.

(2) Die Strafe des Verfalls von Gegenständen (§§ 10, 17 und 18 VStG), die mit einer Verwaltungsübertretung gemäß Abs. 1 in Zusammenhang stehen, kann ausgesprochen werden.

(3) Örtlich zuständig für Entscheidungen nach Abs. 1 und 2 ist jene Behörde, in deren Sprengel die Tat begangen worden ist.

Part VI
Penal provisions

Prohibited processing of source PINs or sector-specific personal identifiers or prohibited use of official signatures

§ 22. (1) Insofar as an act does not carry a more severe penalty in accordance with other provisions on administrative offences, an administrative offence which may be penalised by the local administrative authority with a fine of up to EUR 20,000 is committed by any person who:

1. contrary to the provisions of Part II or III, obtains the source identification number or sector-specific personal-identifier of a natural person with a view to using them in order to acquire unlawfully personal data of the data subject; or
2. stores or uses an sector-specific personal identifier of another private-sector controller without authorisation; or
3. makes available to other private-sector controllers the sector-specific personal identifiers derived from his own source identification number in a prohibited manner; or
4. as a private-sector controller uses a sector-specific personal identifier in order to supply third parties with personal data concerning a registered domicile of the data subject; or
5. uses or purports to use an official signature contrary to § 19(2).

(2) The penalty of forfeit of objects (§ 10, § 17 and § 18 of the Administrative Penal Act) which have been acquired in connection with an administrative offence within the meaning of subparagraph 1 may be imposed.

(3) The authority in whose district the offence was committed shall have territorial jurisdiction to give decisions under subparagraphs 1 and 2.

7. Abschnitt
Übergangs- und Schlussbestimmungen

Sprachliche Gleichbehandlung

§ 23. Soweit in diesem Artikel auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

Inkrafttreten

§ 24. (1) Dieses Bundesgesetz tritt mit Ausnahme seines 4. Abschnitts mit 1. März 2004 in Kraft. Der 4. Abschnitt tritt mit 1. Jänner 2005 in Kraft.

(2) Das Inhaltsverzeichnis, § 1 Abs. 3, § 2 Z 8 und 10, § 3 Abs. 1, § 5, § 6 Abs. 2 bis 6, § 7 Abs. 2, § 8, die Paragrafenüberschrift vor § 9, § 9 Abs. 1 und 2, die Paragrafenüberschrift vor § 10, § 10 Abs. 1 bis 3, die Paragrafenüberschrift vor § 11, § 11, § 12 Abs. 1 Z 4 und Abs. 2, die Paragrafenüberschrift vor § 13, § 13 Abs. 1 bis 3, die Paragrafenüberschrift vor § 14, § 14 Abs. 1 und 2, die Paragrafenüberschrift vor § 15, § 15 Abs. 1 und 2, § 19 Abs. 1 bis 3, § 20, die Paragrafenüberschrift vor § 22, § 22 Abs. 1 Z 1 bis 4 und § 25 Abs. 1 bis 3 in der Fassung des Bundesgesetzes BGBl. I Nr. 7/2008 treten mit 1. Jänner 2008 in Kraft; gleichzeitig tritt § 2 Z 3 außer Kraft.

(3) Das Inhaltsverzeichnis, die Überschrift zu § 17 und § 17 Abs. 2 in der Fassung des Budgetbegleitgesetzes 2011, BGBl. I Nr. 111/2010, tritt mit 1. Jänner 2011 in Kraft. § 17 Abs. 2 in der Fassung des genannten Bundesgesetzes ist von Behörden bei Vorliegen der technischen und organisatorischen Voraussetzungen bei der Behörde und dem Verantwortlichen des betreffenden Registers, spätestens jedoch ab dem 31. Dezember 2012, anzuwenden.

(4) Das Inhaltsverzeichnis, die Abschnittsüberschrift des 2. Abschnitts, § 2 Z 1, 4, 10 und 11, § 2a, § 4 Abs. 2, § 6 Abs. 4 und 6, § 7 Abs. 1, § 8, die Paragrafenüberschrift vor § 9, § 10 Abs. 2, die Abschnittsüberschrift des 3. Abschnitts, § 14 Abs. 1, § 14a, § 16 Abs. 2, § 17 Abs. 2 und Abs. 3 Z 2, § 19 Abs. 1 und 3, § 22 Abs. 1 und 2, die Paragrafenüberschrift vor § 24 und die Paragrafenüberschrift vor § 26 in der Fassung des Bundesgesetzes BGBl. I Nr. 50/2016 treten mit 1. Juli 2016 in Kraft. Gleichzeitig treten § 2 Z 6 und § 25 samt Überschrift außer Kraft.

Part VII
Transitional and final provisions

Gender neutral language

§ 23. To the extent that, in this Article, personal nouns and pronouns are written in male form only, they shall refer equally to women and men.

Entry into force

§ 24. (1) With the exception of Part IV, this federal act shall enter into force on 1 March 2004. Part IV shall enter into force on 1 January 2005.

(2) The table of contents, § 1 (3), § 2 Nos. 8 and 10, § 3 (1), § 5, § 6 (2) to (6), § 7 (2), § 8, the heading before § 9, § 9 (1) and (2), the heading before § 10, § 10 (1) to (3), the heading before § 11, § 11, § 12 (1) No. 4 and (2), the heading before § 13, § 13 (1) to (3), the heading before § 14, § 14 (1) and (2), the heading before § 15, § 15 (1) and (2), § 19 (1) to (3), § 20, the heading before § 22, § 22 (1) Nos. 1 to 4 and § 25 (1) to (3) as amended by the federal act Federal Law Gazette I No. 7/2008 shall enter into force on 1 January 2008; at the same time § 2 No. 3 shall expire.

(3) The table of contents, the heading of §17 and §17 (2) as amended by the Budget Accompanying Act 2011, Federal Law Gazette I No. 111/2010, shall enter into force on 1 January 2011. Authorities shall apply § 17 (2) as amended by the mentioned federal act if the authority and the controller of the respective register meet the technical and organisational requirements, but no later than from 31 December 2012.

(4) The table of contents, the heading of Part II, § 2 Nos. 1, 4, 10 and 11, § 2a, § 4 (2), § 6 (4) and (6), § 7 (1), § 8, the headings before § 9, § 10 (2), the heading of Part III, § 14 (1), § 14a, § 16 (2), § 17 (2) and (3) No. 2, § 19 (1) and (3), § 22 (1) and (2), the heading before § 24 and the heading before § 26 as amended by the federal act Federal Law Gazette I No. 50/2016 shall enter into force on 1 July 2016. At the same time § 2 No. 6 and § 25 with heading shall expire.

(5) Das Inhaltsverzeichnis, die Überschrift des 2. Abschnitts, § 2 Z 11, § 4 Abs. 5, § 6 Abs. 2, § 10 Abs. 2 letzter Satz und Abs. 3, § 13 Abs. 2 erster Satz, § 15 Abs. 1, 1a und 2 letzter Satz, die Überschrift zu § 17, § 17 Abs. 2 letzter Satz, § 21 Abs. 3 und § 25 samt Überschrift in der Fassung des Deregulierungsgesetzes 2017, BGBl. I Nr. 40/2017, treten mit Ablauf des Tages der Kundmachung des genannten Bundesgesetzes in Kraft. § 1a samt Überschrift in der Fassung des genannten Bundesgesetzes tritt mit 1. Jänner 2020 in Kraft. § 1b samt Überschrift in der Fassung des genannten Bundesgesetzes tritt mit Beginn des siebenten auf den Tag der Kundmachung der Verfügbarkeit des Anzeigemoduls gemäß § 37b Abs. 8 des Zustellgesetzes folgenden Monats in Kraft (Anm.: 1).

(6) Das Inhaltsverzeichnis, die Überschrift des 2. Abschnitts, § 2 Z 10, die §§ 4, 4a, 4b und 5 samt Überschriften, § 6 Abs. 1, 4 und 5, § 7 Abs. 2, § 8 erster Satz, § 10 samt Überschrift, § 12, die Überschrift des 3. Abschnitts, § 14 Abs. 1 und 3, § 14a samt Überschrift, § 15, § 18 samt Überschrift, der 5. Abschnitt, § 25 Abs. 2 und 3 und § 28 Z 1 und 4 treten mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft und finden mit Ausnahme von § 25 Abs. 2 und 3 erst Anwendung, wenn die technischen und organisatorischen Voraussetzungen für den Echtbetrieb des E-ID vorliegen. Dieser Zeitpunkt ist vom Bundesminister für Inneres im Bundesgesetzblatt kundzumachen.

(7) Die Einträge im Inhaltsverzeichnis zu den §§ 8, 14, 15 bis 18 und 22, § 3, § 4 Abs. 1, 2, 4, 5 und 6, § 4a Abs. 3 bis 5, § 4b, § 5 Abs. 1 bis 3, § 6 Abs. 2 und 4, § 7 Abs. 2, § 8 samt Überschrift, § 9 Abs. 1 und 2, § 10 Abs. 1 und 2, § 11, § 12, § 13, § 14 samt Überschrift, § 14a Abs. 2, die Überschrift zu § 15, § 15 Abs. 1, die Überschrift zu § 16, § 16 Abs. 2, § 17 samt Überschrift, die Überschrift zu § 18, § 18 Abs. 1 und 2, § 19 Abs. 2 und 3, die Überschrift zu § 22, § 22 Abs. 1, § 24 Abs. 3 sowie § 25 Abs. 2 in der Fassung des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 32/2018, treten mit 25. Mai 2018 in Kraft und finden mit Ausnahme des Eintrags im Inhaltsverzeichnis zu § 22 und von § 3, § 6 Abs. 2, § 9 Abs. 1 und 2, § 11, § 13, der Überschrift zu § 16, § 16 Abs. 2, § 17 samt Überschrift, § 19 Abs. 2 und 3, der Überschrift zu § 22, § 22 Abs. 1, § 24 Abs. 3 und § 25 Abs. 2 erst ab dem Zeitpunkt Anwendung, den der Bundeminister für Inneres gemäß Abs. 6 letzter Satz im Bundesgesetzblatt kundmacht. § 6 Abs. 5 in der Fassung des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 32/2018, tritt mit dem vom Bundesminister für Inneres gemäß Abs. 6 im Bundesgesetzblatt kundgemachten Zeitpunkt in Kraft.

(8) § 4 Abs. 8, § 4a Abs. 6, § 5 Abs. 1, § 6 Abs. 4, § 7, § 9 Abs. 1 und 2, § 10 Abs. 2, die Überschrift zu § 14, die Überschrift zu § 15 sowie § 15 Abs. 1 Z 2, § 18

(5) The table of contents, the heading of Part II, § 2 No. 11, § 4 (5), § 6 (2), § 10 (2) last sentence and (3), § 13 (2) first sentence, § 15 (1), (1a) and (2) last sentence, the heading of § 17, § 17 (2) last sentence, § 21 (3) and § 25 with heading as amended by Deregulation Act 2017, Federal Law Gazette I No. 40/2017 shall enter into force at the end of the date of promulgationof the mentioned federal act. § 1a with heading as amended by the mentioned federal act shall enter into force on 1 January 2020. § 1b with heading as amended by the mentioned federal act shall enter into force with the beginning of the seventh month after the day of the publication of the availability of the indicate module corresponding to § 37b (8) of the Service of Documents Act.

(6) The table of contents, the heading of Part II, § 2 No. 10, § 4, § 4a, § 4b and § 5 including the headings, § 6 (1), (4) and (5), § 7 (2), § 8 first sentence, § 10 including the heading, § 12, the heading of Part III, § 14 (1) and (3), § 14a including the heading, § 15, § 18 including the heading, Part V, § 25 (2) and (3) and § 28 Nos. 1 and 4 shall enter into force at the end of the date of promulgation of this federal act and, with the exception of § 25 (2) and (3), shall apply only if the technical and organisational requirements of live operation of the eID are met. The Federal Minister of the Interior shall announce this date in the Federal Law Gazette.

(7) The entries in the table of contents regarding § 8, § 14, § 15 to § 18 and § 22, § 3, § 4 (1), (2), (4), (5) and (6), § 4a (3) to (5), § 4b, § 5 (1) to (3), § 6 (2) and (4), § 7 (2), § 8 including the heading, § 9 (1) and (2), § 10 (1) and (2), § 11, § 12, § 13, § 14 including the heading, § 14a (2), the heading of § 15, § 15 (1), the heading of § 16, § 16 (2), § 17 including the heading, the heading of § 18, § 18 (1) and (2), § 19 (2) and (3), the heading of § 22, § 22 (1), § 24 (3) as well as § 25 (2) as amended by the Substantive Law (Data Protection) Amendment Act 2018, Federal Law Gazette I No. 32/2018, shall enter into force on 25 May 2018 and, with the exception of the entry in the table of contents regarding § 22 and of § 3, § 6 (2), § 9 (1) and (2), § 11, § 13, the heading of § 16, § 16 (2), § 17 including the heading, § 19 (2) and 3, the heading of § 22, § 22 (1), § 24 (3) and § 25 (2), shall apply only from the date which the Federal Minister of the Interior announces in the Federal Law Gazette pursuant to subparagraph 6 last sentence. § 6 (5) as amended by the Substantive Law (Data Protection) Amendment Act 2018, Federal Law Gazette I No. 32/2018, shall enter into force on the date announced by the Federal Minister of the Interior in the Federal Law Gazette pursuant to subparagraph 6 last sentence.

(8) § 4 (8), § 4a (6), § 5 (1), § 6 (4), § 7, § 9 (1) and (2), § 10 (2), the heading of § 14, the heading of § 15 as well as § 15 (1) No. 2, § 18 (3), § 19 (2), § 25 (3) and

Abs. 3, § 19 Abs. 2, § 25 Abs. 3 und § 28 Z 1 bis 3 und 4a in der Fassung des Bundesgesetzes BGBl. I Nr. 104/2018 treten mit Ablauf des Tages der Kundmachung in Kraft und finden mit Ausnahme von § 7 Abs. 1, § 9 Abs. 1 und 2, § 19 Abs. 2, § 25 Abs. 3 und § 28 Z 2, 3 und 4a erst ab dem Zeitpunkt Anwendung, den der Bundesminister für Inneres gemäß Abs. 6 letzter Satz im Bundesgesetzblatt kundmacht. § 6 Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 104/2018 tritt am 29. September 2018 in Kraft und mit dem vom Bundesminister für Inneres gemäß Abs. 6 im Bundesgesetzblatt kundgemachten Zeitpunkt wieder außer Kraft. § 1 Abs. 3 tritt mit Ablauf des 22. September 2020 außer Kraft.

(Anm. 1: Die Kundmachung erfolgte am 30.5.2018 mit BGBl. I Nr. 33/2018.)

Übergangsbestimmung

§ 25. (1) Die Gerichte und Verwaltungsbehörden, deren Einrichtung in Gesetzgebung Bundessache ist, sind verpflichtet, bis spätestens 1. Jänner 2020 die technischen und organisatorischen Voraussetzungen für einen elektronischen Verkehr mit den Beteiligten gemäß § 1a zu schaffen.

(2) Ab der Kundmachung des Bundesgesetzes, BGBl. I Nr. 121/2017, dürfen zur Gewährleistung eines sicheren Betriebes für die vollumfängliche Nutzung des E-ID unter Anwendung der dafür erforderlichen Bestimmungen dieses Bundesgesetzes zeitlich, örtlich oder auf bestimmte Personengruppen beschränkte Pilotbetriebe unter Verarbeitung personenbezogener Daten durchgeführt werden, sofern die Betroffenen daran freiwillig mitwirken.

(3) Sofern die technischen und organisatorischen Voraussetzungen zum Echtbetrieb des E-ID gemäß der Kundmachung nach § 24 Abs. 6 noch nicht vorliegen, ist für bis zum Zeitpunkt der Aufnahme des Echtbetriebes ausgestellte Bürgerkarten die Rechtslage vor Inkrafttreten dieses Bundesgesetzes, BGBl. I Nr. 121/2017, anzuwenden. Der Bundesminister für Inneres ist im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort ermächtigt, mit Verordnung für Bürgerkarteninhaber einen vereinfachten Prozess für den Umstieg von der Bürgerkarte auf einen E-ID vorzusehen.

Erlassung und Inkrafttreten von Verordnungen

§ 26. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

§ 28 Nos. 1 to 3 and 4a as amended by the federal act Federal Law Gazette I No. 104/2018 shall enter into force at the end of the date of promulgation and, with the exception of § 7 (1), § 9 (1) and (2), § 19 (2), § 25 (3) and § 28 Nos. 2, 3 and 4a, shall apply only from the date which the Federal Minister of the Interior announces in the Federal Law Gazette pursuant to subparagraph 6 last sentence. § 6 (5) as amended by the federal act Federal Law Gazette I No. 104/2018 shall enter into force on 29 September 2018 and shall expire on the date announced by the Federal Minister of the Interior in the Federal Law Gazette pursuant to subparagraph 6. § 1 (3) shall expire at the end of 22 September 2020.

(Note 1: promulgated on 30 May 2018 in Federal Law Gazette I No. 33/2018.)

Transitional provisions

§ 25. (1) The courts and administrative bodies, which are established by federal legislation, are forced to create the technical and organizational requirements for an electronic communication with the involved parties corresponding to § 1a.

(2) Following promulgation of the federal act promulgated in Federal Law Gazette I No. 121/2017, trial operations including the processing of personal data and limited in terms of time, place or to certain groups of persons may be carried out to ensure safe operations for the full use of the eID, applying the provisions of this federal act required for this purpose provided that the data subjects cooperate voluntarily.

(3) If the technical and organisational requirements of live operation of the eID have not yet been met in accordance with the announcement pursuant to § 24 (6), the legal provisions applicable before the entry into force of this federal act, Federal Law Gazette I No. 121/2017, shall be applied to citizen cards issued until the start of live operations. The Federal Minister of the Interior, with the consent of the Federal Minister of Digital and Economic Affairs, is authorised to enact, by regulation, a simplified procedure for holders of citizen cards to transfer from the citizen card to the eID.

Adoption and entry into force of regulations

§ 26. Regulations based on this federal act, as it may be amended, may be adopted from the day following proclamation of the statutory provisions to be implemented by them; however, they may not enter into force before those statutory provisions.

Verweisungen

§ 27. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 28. Mit der Vollziehung dieses Bundesgesetzes sind betraut:

1. hinsichtlich des § 4 Abs. 8 der Bundesminister für Digitalisierung und Wirtschaftsstandort im Einvernehmen mit dem Bundesminister für Inneres sowie den allfällig sonst zuständigen Bundesministern,
2. hinsichtlich des § 7 Abs. 2 der Bundesminister für Digitalisierung und Wirtschaftsstandort im Einvernehmen mit dem Bundesminister für Inneres, dem Bundesminister für Finanzen oder dem Bundeskanzler, je nachdem, ob es sich um Dienstleistungen betreffend Stammzahlen natürlicher Personen oder um Dienstleistungen betreffend Stammzahlen nicht-natürlicher Personen handelt und welches Auftragsverarbeiters sich der Bundesminister für Digitalisierung und Wirtschaftsstandort dabei bedient,
3. hinsichtlich des § 9 Abs. 2 der Bundesminister für Digitalisierung und Wirtschaftsstandort,
4. hinsichtlich des § 4a Abs. 1 bis 5, des § 4b, des § 17 Abs. 1 und 3 sowie des § 18 Abs. 1 und 2 der Bundesminister für Inneres,

4a. hinsichtlich des § 4a Abs. 6, des § 18 Abs. 3 und des § 25 Abs. 3 der Bundesminister für Inneres im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort,

5. hinsichtlich des § 16 der Bundesminister für Finanzen,
6. im übrigen, soweit sie nicht der Bundesregierung oder den Landesregierungen obliegt, jeder Bundesminister im Rahmen seines Wirkungsbereiches.

References

§ 27. Insofar as reference is made in this federal act to other federal acts, those acts shall be applicable in the version in force at the relevant time.

Implementation

§ 28. The following shall be competent to implement this federal act:

1. with respect to § 4 (8), the Federal Minister of Digital and Economic Affairs acting with the consent of the Federal Minister of the Interior and any other competent Federal Ministers,
2. with respect to § 7 (2), the Federal Minister of Digital and Economic Affairs acting with the consent of the Federal Minister of the Interior, the Federal Minister of Finance or the Federal Chancellor, depending on whether services relating to the source identification numbers of natural persons or services relating to the source identification numbers of non-natural persons are concerned and which processor the Federal Minister of Digital and Economic Affairs uses for that purpose,
3. with respect to § 9 (2), the Federal Minister of Digital and Economic Affairs,
4. with respect to § 4a (1) to (5), § 4b, § 17 (1) and (3) as well as § 18 (1) and (2), the Federal Minister of the Interior,

4a. with respect to § 4a (6), § 18 (3) and § 25 (3), the Federal Minister of the Interior acting with the consent of the Federal Minister of Digital and Economic Affairs,

5. with respect to § 16, the Federal Minister of Finance,
6. as regards the remainder, any Federal Minister within his area of competence and to the extent that implementation is not a matter for the Federal Government or the Provincial Governments.