

**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.](#))

[BGBl. I Nr. 169/2020](#) (NR: GP XXVII [RV 469 AB 495 S. 69](#). BR: [AB 10480 S. 916.](#))

[BGBl. I Nr. 119/2022](#) (NR: GP XXVII [RV 1443 AB 1636 S. 167](#). BR: [AB 11042 S. 943.](#))

[BGBl. I Nr. 117/2024](#) (NR: GP XXVII [IA 4092/A AB 2664 S. 272](#). BR: [AB 11584 S. 970.](#))

**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 [F. L. G. = BGBl.])

← 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.

## Inhaltsverzeichnis

### 1. Abschnitt Gegenstand und Ziele des Gesetzes

- § 1.
- § 1a. Recht auf elektronischen Verkehr und Wahlfreiheit zwischen Kommunikationsarten für Bürgerinnen und Bürger
- § 1b. Teilnahme an der elektronischen Zustellung durch Unternehmen
- § 1c. Elektronischer Verkehr zwischen Verantwortlichen des öffentlichen Bereichs

### 2. Abschnitt Eindeutige Identifikation und die Funktion E-ID

- § 2. Begriffsbestimmungen
- § 2a.
- § 3. Identität und Authentizität
- § 4. Die Funktion E-ID
- § 4a. Registrierung und Widerruf des E-ID
- § 4b. Registrierungsdaten
- § 5. E-ID und Stellvertretung
- § 6. Stammzahl
- § 6a. Ergänzungsregister für natürliche Personen
- § 6b. Ergänzungsregister für sonstige Betroffene
- § 7. Stammzahlenregisterbehörde
- § 8. Eindeutige Identifikation in Datenverarbeitungen
- § 9. Bereichsspezifisches Personenkennzeichen (bPK)
- § 10. Erzeugung und Anforderung von bPK und Stammzahlen nicht-natürlicher Personen
- § 11. Offenlegung von bPK in Mitteilungen
- § 12. Schutz der Stammzahl natürlicher Personen
- § 13. Weitere Garantien zum Schutz von bPK

## Table of contents

### Part I Object and aims of the act

- § 1.
- § 1a. Right to electronic communications and citizens' freedom of choice between different means of communication
- § 1b. Participation in electronic delivery by businesses
- § 1c. Electronic communications between public-sector controllers

### Part II Unique identification and the eID function

- § 2. Definitions
- § 2a.
- § 3. Identity and authenticity
- § 4. The eID function
- § 4a. Registration and revocation of the eID
- § 4b. Registration data
- § 5. eID and representation
- § 6. Source PIN
- § 6a. Supplementary Register for Natural Persons
- § 6b. Supplementary Register for Other Data Subjects
- § 7. Source PIN Register Authority
- § 8. Unique identification in data processing systems
- § 9. Sector-specific personal identifiers
- § 10. Generation and requirements of sector-specific personal identifiers and source PIN of non-natural persons
- § 11. Disclosure of sector-specific personal identifiers in communications
- § 12. Protection of the source PIN of natural persons
- § 13. Further guarantees for the protection of sector-specific personal identifiers

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

- § 14. Erzeugung von bPK für die Verwendung des E-ID im privaten Bereich
- § 14a. E-ID-taugliche Anwendungen im Ausland
- § 15. Garantien zum Schutz der Stammzahl und der bPK bei der Verarbeitung im privaten Bereich

**4. Abschnitt**  
**Elektronischer Datennachweis**

- § 16. für personenbezogene Daten über selbständige wirtschaftliche Tätigkeiten
- § 17. für personenbezogene Daten aus Registern
- § 18. über personenbezogene Daten aus elektronischen Registern eines Verantwortlichen des öffentlichen oder privaten Bereichs

**5. Abschnitt**  
**Besonderheiten elektronischer Aktenführung**

- § 19. Amtssignatur
- § 20. Beweiskraft von Ausdrucken
- § 20a. Ersetzendes Scannen
- § 21. Vorlage elektronischer Akten

**5a. Abschnitt**  
**Haftungsbestimmungen**

- § 21a. Haftung

**6. Abschnitt**  
**Strafbestimmungen**

- § 22. Unzulässige Verarbeitung von Stammzahlen oder bPK oder unzulässige Verwendung von Amtssignaturen

**7. Abschnitt**  
**Übergangs- und Schlussbestimmungen**

- § 23. Sprachliche Gleichbehandlung
- § 24. Inkrafttreten

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

- § 14. Generation of sector-specific personal identifiers for use of the eID in the private sector
- § 14a. eID-compatible applications abroad
- § 15. Guarantees for the protection of source PIN and sector-specific personal identifiers when processed in the private sector

**Part IV**  
**Electronic validation of data**

- § 16. for personal data on economic activities as a self-employed person
- § 17. for personal data from registers
- § 18. regarding personal data from electronic registers of a public-sector or private-sector controller

**Part V**  
**Special characteristics of keeping electronic records**

- § 19. Official signature
- § 20. Probative value of printouts
- § 20a. Substitute scanning
- § 21. Submission of the electronic records

**Part Va**  
**Liability provisions**

- § 21a. Liability

**Part VI**  
**Penal provisions**

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

**Part VII**  
**Transitional and final provisions**

- § 23. Gender-neutral language
- § 24. Entry into force

- § 25. Übergangsbestimmung
- § 26. Erlassung und Inkrafttreten von Verordnungen
- § 27. Verweisungen
- § 28. Vollziehung

## 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.

*(Anm.: Abs. 3 aufgehoben durch Art. 1 Z 1, BGBl. I Nr. 104/2018)*

### Recht auf elektronischen Verkehr und Wahlfreiheit zwischen Kommunikationsarten für Bürgerinnen und Bürger

§ 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.

- § 25. Transitional provisions
- § 26. Adoption and entry into force of regulations
- § 27. References
- § 28. Implementation

## 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 para 1 and implemented where other precautions do not already provide adequate protection.

*(Note: para 3 repealed by Article 1 subpara 1, Federal Law Gazette I No. 104/2018)*

### Right to electronic communications and citizens' freedom of choice between different means of communication

§ 1a. (1) Everyone has the right to electronic communications with courts and administrative authorities in matters of federal legislation, except in matters which are not suitable to be dealt with electronically. Persons serving a prison sentence handed down by a court, a financial penal authority or an administrative authority pursuant to § 53d of the [Administrative Penal Act 1991](#), Federal Law Gazette No. 52/1991, can only exercise this right where the related technical and organisational conditions in penitentiaries so permit, provided that this is permissible under law enforcement standards and unlikely to pose a threat to safety and order.

(2) Any technical requirements or organisational restrictions of electronic communications as well as the time of commencement of electronic communications shall be announced on the Internet.

(3) Sofern durch Bundesgesetz nichts anderes geregelt ist, ist neben der Möglichkeit des elektronischen Verkehrs zumindest eine andere Kommunikationsart für den Verkehr mit der jeweiligen Stelle vorzusehen. Benachteiligungen von Personen auf Grund der Wahl dieser anderen Kommunikationsart sind unzulässig. Maßnahmen zur Förderung des elektronischen Verkehrs stellen keine Benachteiligung in diesem Sinne dar.

#### **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. 163/1999, 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.

#### **Elektronischer Verkehr zwischen Verantwortlichen des öffentlichen Bereichs**

§ 1c. Verantwortliche des öffentlichen Bereichs, die durch Bundesgesetz eingerichtet sind, sind untereinander zum elektronischen Verkehr verpflichtet. Ausgenommen sind Angelegenheiten, die nicht geeignet sind, elektronisch besorgt zu werden.

## **2. Abschnitt**

### **Eindeutige Identifikation und die Funktion E-ID**

#### **Begriffsbestimmungen**

§ 2. Im Sinne dieses Bundesgesetzes bedeutet

(3) Unless otherwise provided for by federal legislation, at least one other means of communication shall be provided for communication with the relevant body in addition to the option of electronic communication. No person shall be disadvantaged due to their choice of such other means of communication. Measures to promote electronic communication shall not be construed as placing any person at a disadvantage in this sense.

#### **Participation in electronic delivery by businesses**

§ 1b. (1) Businesses within the meaning of § 3 subpara 20 of the Federal Act on Federal Statistics (Federal Statistics Act 2000), Federal Law Gazette I No. 163/1999, shall participate in electronic delivery.

(2) Participation in electronic delivery is unacceptable if the business does not have the necessary technical requirements or an Internet connection.

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

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

#### **Electronic communications between public-sector controllers**

§ 1c. Public-sector controllers established by federal legislation are obligated to use electronic communications in dealings with each other, except in matters that are not suitable to be dealt with electronically.

## **Part II**

### **Unique identification and the eID function**

#### **Definitions**

§ 2. For the purposes of this Federal Act, the following definitions shall apply:

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)numerische 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 (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen verbindet;
  - 10a. „Verwendung des E-ID“: das Auslösen der Erstellung einer Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers oder mittels eines sicherheitstechnisch gleichwertigen Vorgangs, der an eine frühere qualifizierte elektronische Signatur des E-ID-Inhabers gebunden ist, wobei das zugehörige qualifizierte Zertifikat, das für die
1. “Identity”: designation of a specific data subject (subpara 7) by means of data which are suitable to distinguish data subjects 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 data subject (subpara 7) by means of one or more data enabling that data subject to be unmistakably distinguished from all other data subjects;  
(Note: subpara 3 repealed by Federal Law Gazette I No. 7/2008)
  4. “Unique identification”: electronic identification pursuant to Art. 3 subpara 1 of the eIDAS Regulation (subpara 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: subpara 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 PIN;
  10. “Electronic proof of identity (eID)”: a logical unit that, independent of its technical implementation combines a qualified electronic signature (Art. 3 subpara 12 of the eIDAS Regulation) with an identity link (§ 4 para 2) and the associated security data and functions.
  - 10a. “Use of the eID”: the triggering of the creation of an identity link by means of a qualified electronic signature of the eID holder or by means of an alternative procedure providing the same degree of security that is linked to a past qualified electronic signature of the eID holder, provided that the related qualified certificate used for the past qualified electronic signature is still valid at the time of use;

frühere qualifizierte elektronische Signatur verwendet wurde, zum Zeitpunkt der jeweiligen Verwendung noch gültig sein muss;

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 Personenbindung bewirkt: Von der Stammzahlenregisterbehörde (§ 7) wird

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 subpara 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 “GDPR”) in connection with § 26 para 1 of the [Data Protection Act](#), Federal Law Gazette I No. 165/1999, rights of access to personal data (Art. 4 subpara 1 of the GDPR) 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 data subject 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 data 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 identity link: the Source PIN Register Authority (§ 7) shall confirm, by electronic

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. Für Zwecke der mittels eines sicherheitstechnisch gleichwertigen Vorgangs im Sinne des § 2 Z 10a zweiter Fall ausgelösten Erstellung einer Personenbindung, ist die verschlüsselte Stammzahl zum E-ID dieses E-ID-Inhabers zu speichern.

(5) Verwendet der E-ID-Inhaber den 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. Wird die Erstellung der Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers

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 subparas 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 subpara 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 subparas 1 to 4, 7, 10 and 11 and any limitation of the period of validity of the certificate pursuant to § 4a para 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. For the purposes of the creation of an identity link triggered by means of an alternative procedure providing the same degree of security as referred to in § 2 subpara 10a second case, the encrypted source PIN associated with the eID of the relevant eID holder must be stored.

(5) If the eID holder uses the eID in electronic communications pursuant to § 10 para 1, the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (para 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. If the creation of the identity link is triggered by means of a qualified electronic signature of the eID holder (§ 2

ausgelöst (§ 2 Z 10a erster Fall), hat der qualifizierte VDA die verschlüsselte Stammzahl und die zugehörigen Sicherheitsdaten 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 oder privaten Bereichs eingefügt werden.

(6) Nach Maßgabe der technischen Möglichkeiten kann der E-ID-Inhaber Vorname, Familienname, Geburtsdatum und den Bestand weiterer Merkmale gemäß Abs. 5 letzter Satz einem Dritten gegenüber in vereinfachter Form nachweisen. Zu diesem Zweck können Vorname, Familienname, Geburtsdatum und die weiteren Merkmale für einen begrenzten Zeitraum zu seinem E-ID gespeichert werden. Vorname, Familienname, Geburtsdatum dürfen für längstens zwölf Monate gespeichert werden. Ob und für welchen Zeitraum dies für ein bestimmtes weiteres Merkmal zulässig ist, hat jener Verantwortliche des öffentlichen Bereichs festzulegen, der das Register führt, aus dem die Stammzahlenregisterbehörde dieses Merkmal bezogen hat. Einem vereinfachten Nachweis von Vorname, Familienname, Geburtsdatum und Lichtbild der betreffenden Person als weiteres Merkmal kommt in den Angelegenheiten, die in Gesetzgebung Bundessache sind, die Beweiskraft eines amtlichen Lichtbildausweises gemäß § 6 Abs. 2 Z 1 des Finanzmarkt-Geldwäschegesetzes – FM-GwG, BGBl. I Nr. 118/2016, zu.

(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

subpara 10a first case), the qualified TSP shall provide to the Source PIN Register Authority the encrypted source PIN and the associated security data. In accordance with the technical possibilities, further data of the eID holder taken from registers of public-sector or private-sector controllers which the 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 his first name, family name, date of birth and the existence of further data pursuant to para 5 last sentence to a third party in a simplified form. For this purpose, the first name, family name, date of birth and further data can be stored on the eID holder's eID for a limited period. The first name, family name and date of birth may be stored for a maximum period of twelve months. 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 further data. Simplified proof of a person's first name, family name, date of birth and photograph as a piece of further data shall, in matters of federal legislation, have the probative value of an official photo identification document pursuant to § 6 para 2 subpara 1 of the Financial Markets Anti-Money Laundering Act, Federal Law Gazette I No. 118/2016.

(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 paras 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 para 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

§ 16 Abs. 3 des Passgesetzes 1992 ermächtigen 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 zum Inland verfügen und das 14. Lebensjahr vollendet haben. Insbesondere ist hierfür 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 gemäß dem Passgesetz 1992, dessen Gültigkeitsdauer nicht länger als sechs Jahre abgelaufen ist, den Behörden im Wege des VDA (§ 4 Abs. 4 erster Satz), der im Auftrag des Auftragsverarbeiters der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 tätig wird, bereits vorweg die Namen, das Geburtsdatum, die Pass- oder Personalausweisnummer und soweit verfügbar eine E-Mail-Adresse 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. In den Fällen des Abs. 1 zweiter Satz und Abs. 2 ist für die Registrierung eines E-ID ein Lichtbild beizubringen, das den Anforderungen gemäß § 4 der Passgesetz-Durchführungsverordnung (PassG-DV), BGBl. II Nr. 223/2006, in der Fassung der Verordnung BGBl. II Nr. 184/2023, entspricht, es sei denn der Registrierungsbehörde liegt bereits ein Lichtbild in der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 vor, das nicht für die Ausstellung eines Reisepasses gemäß § 4a des Passgesetzes 1992 vorgelegt wurde.

pursuant to § 16 para 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 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 subpara 15 of the eIDAS Regulation may be valid for a maximum of three years from the time of registration. Para 1 penultimate and last sentences shall apply to foreigners *mutatis mutandis*.

(3) To the extent that holders of an Austrian travel document pursuant to the Passport Act 1992 which expired not more than six years ago provide to the authorities, through the TSP (§ 4 para 4 first sentence) acting on behalf of the processor of the data processing system pursuant to § 22b of the Passport Act 1992, their names, date of birth, passport or identity card number and, if available, an email address in advance, the authorities may store these data for further processing for 30 days for the purpose of the 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. In the cases of para 1 second sentence and para 2, a photograph that meets the requirements of § 4 of the Passport Act Implementing Regulation, Federal Law Gazette II No. 223/2006, as amended by the regulation Federal Law Gazette II No. 184/2023, must be provided in order to register an eID, unless a photograph is already available to the registering authority in the data processing system pursuant to § 22b of the Passport Act 1992 and such photograph was not provided for the purpose of issuing a passport pursuant to § 4a of the Passport

Zur Überprüfung der Identität und der vorgelegten Dokumente ist die Behörde ermächtigt, Informationen über personenbezogene Daten und Dokumente des E-ID-Werbers aus Datenverarbeitungen von Sicherheits-, Personenstands- und Staatsbürgerschaftsbehörden sowie aus Datenverarbeitungen nach den §§ 26 und 27 des BFA-Verfahrensgesetzes (BFA-VG), BGBl. I Nr. 87/2012, im Datenfernverkehr abzufragen und soweit es sich um Daten gemäß § 4b Abs. 1 Z 1 bis 5 oder Z 7 handelt, in der Datenverarbeitung gemäß § 22b des Passgesetzes 1992 zu verarbeiten. 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 über die Vorgangsweise gemäß Abs. 1 bis 5 sowie für die Verlängerung der Gültigkeit eines E-ID durch Verordnung festzulegen.

#### **Registrierungsdaten**

§ 4b. (1) Die mit der Registrierung des E-ID betrauten Behörden sind ermächtigt als Verantwortliche

1. die Namen,
2. das Geburtsdatum,
3. den Geburtsort,
4. das Geschlecht,
5. die Staatsangehörigkeit,
6. das bPK,

Act 1992. To verify the identity and the documents provided, the authority is authorised to retrieve, via electronic communications, information on personal data and documents of the eID applicant from data processing systems of security authorities, civil status authorities and nationality authorities as well as from data processing systems pursuant to § 26 and § 27 of the Act on Procedures before the Federal Office for Immigration and Asylum, Federal Law Gazette I No. 87/2012, and, insofar as data pursuant to § 4b para 1 subparas 1 to 5 or subpara 7 are concerned, process such data in the data processing system pursuant to § 22b of the Passport Act 1992. If an eID applicant cannot be uniquely identified by the authorities pursuant to paras 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 para 3 of the eIDAS Regulation. The TSP shall send the information on the suspension or revocation to the relevant competent authority pursuant to paras 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 paras 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 provisions on the procedure pursuant to paras 1 to 5 and on the extension of the validity of an eID.

#### **Registration data**

§ 4b. (1) 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. die bekanntgegebene Zustelladresse,
8. das aktuelle Lichtbild, ausgenommen das Lichtbild eines Reisepasses gemäß § 4a des Passgesetzes 1992
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.

(2) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 und 3 besteht kein Widerspruchsrecht gemäß Art. 21 DSGVO sowie kein Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Darüber sind die Betroffenen in geeigneter Weise zu informieren.

(3) Die mit der Registrierung des E-ID betrauten Behörden sind ermächtigt, Ausstellungsbehörde, Ausstellungsstaat, Ausstellungsdatum, gegebenenfalls Gültigkeitsdauer, Dokumentenart und -nummer der vorgelegten Urkunden und Nachweise zur eindeutigen Feststellung der Identität gemeinsam mit den darauf Bezug habenden personenbezogenen Daten nach Abs. 1 automatisiert zu verarbeiten.

(4) Protokolldaten über tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, sind drei Jahre lang aufzubewahren.

(5) Die bekanntgegebene Zustelladresse gemäß Abs. 1 Z 7 ist zu löschen, sobald die Registrierung des E-ID abgeschlossen wurde. Gemäß Abs. 1 Z 13 verarbeitete Identitätscodes der ausgestellten Zertifikate sind im Falle eines Widerrufs oder Ablaufs des jeweiligen Zertifikats zu löschen. Sonstige gemäß Abs. 1 und 3 sowie gemäß § 4a Abs. 4 verarbeitete personenbezogene Daten sind

7. the address for service provided,
8. the recent photograph, except for a photograph used in a passport pursuant to § 4a of the Passport Act 1992,
9. the date of registration,
10. if available, the mobile telephone number provided,
11. if available, the email address provided,
12. the registering authority, and
13. the identity code of the certificate issued pursuant to § 4 para 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.

(2) As regards the processing of personal data pursuant to paras 1 and 3, there is no right to object pursuant to Art. 21 of the GDPR and no right to restriction of processing pursuant to Art. 18 of the GDPR. Data subjects must be made aware of this by appropriate means.

(3) The authorities entrusted with registering an eID are authorised to process, by automated means, the issuing authority, the issuing country, the date of issue, the period of validity (if applicable), the document type and the document number of the documents and proof submitted for the purpose of unique identification along with the related personal data pursuant to para 1.

(4) Records of any processing activities actually performed, such as changes, retrievals and transfers of data, must be retained for a period of three years.

(5) The address for service provided pursuant to para 1 subpara 7 must be deleted upon completion of the registration of an eID. Identity codes of the certificates issued that are processed pursuant to para 1 subpara 13 must be deleted if the relevant certificate is revoked or expires. Any other personal data processed pursuant to paras 1 and 3 and pursuant to § 4a para 4 must be deleted as soon as they

zu löschen, sobald sie nicht mehr benötigt werden, jedoch spätestens drei Jahre nach Widerruf oder Ablauf des E-ID.

### **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 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

are no longer needed, but no later than three years after the revocation or expiry of the eID.

### **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 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 para 8. The permission to receive documents pursuant to § 35 para 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 para 1. The general authority does not include the permission according to § 35 para 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 data subject 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 data subjects 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

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 § 14a Abs. 2 gelten für vertretungsweise 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 auf Basis ihrer 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) Unbeschadet des Vorhandenseins einer Stammzahl gemäß Abs. 2 ist als Stammzahl für Betroffene

1. die im Firmenbuch, eingetragen sind, die Firmenbuchnummer (§ 3 Abs. 1 Z 1 des Firmenbuchgesetzes, BGBl. Nr. 10/1991),
2. die im Zentralen Vereinsregister eingetragen sind, die Vereinsregisterzahl (§ 18 Abs. 2 des Vereinsgesetzes 2002, BGBl. I Nr. 66/2002),
3. die ein Unternehmen im Sinne des § 3 Z 20 des Bundesstatistikgesetz 2000, BGBl. I Nr. 163/1999, sind, und

PIN Register Authority shall include the existence of the official's authority in the identity link pursuant to para 1. The general authority does not include the permission according to § 35 para 3 second sentence of the [Service of Documents Act](#) and the authorisation for deliveries according to § 9 para 1 of the [Service of Documents Act](#).

(4) If the existence of sole power of representation is included in the identity link (§ 4 para 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 para 5, § 14 para 3 and § 14a para 2 shall 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 on the basis of his source PIN.

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

(3) Irrespective of the availability of a source PIN pursuant to para 2, the source PIN for data subjects

1. entered in the Register of Company Names shall be the Register of Company Names number (§ 3 para 1 subpara 1 of the Register of Company Names Act, Federal Law Gazette No. 10/1991),
2. entered in the Central Register of Associations shall be the Central Register of Associations number (ZVR number) (§ 18 para 2 of the Associations Act 2002, Federal Law Gazette I No. 66/2002),
3. that qualify as a business within the meaning of § 3 subpara 20 of the Federal Statistics Act 2000, Federal Law Gazette I No. 163/1999, and that

- a) Einkünfte gemäß des § 2 Abs. 3 Z 1 bis 3 und 6 des Einkommensteuergesetzes 1988 – EStG 1988, BGBl. Nr. 400/1988, erzielen,
  - b) keine Gebietskörperschaften oder andere Körperschaften oder Anstalten des öffentlichen Rechts sind sowie
  - c) nicht im Firmenbuch oder im Zentralen Vereinsregister eingetragen sind,
- die für sie vergebene Global Location Number (GLN),
- 4. die ein im land- und forstwirtschaftliches Betriebsinformationssystem (LFBIS) gemäß des § 1 Abs. 1 LFBIS-Gesetz, BGBl. Nr. 448/1980, zu erfassender land- und forstwirtschaftlicher Betrieb sind, und nicht unter Z 1 bis 3 fallen, die für sie vergebene GLN,
  - 5. die die Gründung eines Unternehmens im Sinne des § 3 Z 20 Bundesstatistikgesetz 2000 über ein elektronisches Verfahren begonnen haben und nicht unter Z 1 bis 4 fallen, die für sie vergebene GLN,
  - 6. die im Ergänzungsregister für sonstige Betroffene (Abs. 4) eingetragen sind, die im Ergänzungsregister vergebene Ordnungsnummer zu verwenden.

(3a) Die GLN wird für jeden Betroffenen einmalig für die Dauer seines Bestehens als Betroffener iSd Abs. 3 Z 3 bis 5 vergeben. Ihre Vergabe erfolgt im Fall der Abs. 3 Z 3 im Auftrag der Finanzbehörden des Bundes, im Fall der Abs. 3 Z 4 im Auftrag des für Landwirtschaft, Regionen und Tourismus zuständigen Bundesministers sowie im Fall der Abs. 3 Z 5 im Auftrag des Betreibers des Unternehmensserviceportals (USP) jeweils durch die Bundesanstalt „Statistik Österreich“ im Rahmen der Eintragung in das Unternehmensregister gemäß des § 25 Bundesstatistikgesetz 2000. Tritt an die Stelle des Anlasses der Eintragung ein anderer Anlass iSd Abs. 3 Z 3 bis 5 bleibt die vergebene GLN als Identifikationsmerkmal dieses Betroffenen erhalten und es ist keine neue GLN zu vergeben. Wenn es sich bei einem Betroffenen iSd Abs. 3 Z 1 oder 3 bis 6 um eine natürliche Person handelt, ist die Firmenbuchnummer, GLN oder Ordnungsnummer nur soweit zu verwenden als seine Identität als in das Firmenbuch eingetragener Einzelunternehmer, Unternehmen gemäß des § 3 Z 20 Bundesstatistikgesetz 2000, land- und forstwirtschaftlicher Betrieb, die Identität dieser natürlichen Person in Bezug auf ein begonnenes elektronisches Verfahren zur Gründung eines

- a) generate income pursuant to § 2 para 3 subparas 1 to 3 and 6 of the Income Tax Act 1988, Federal Law Gazette No. 400/1988,
  - b) are not territorial authorities or other corporations or institutions under public law, and
  - c) are not entered in the Register of Company Names or in the Central Register of Associations,
- shall be the Global Location Number (GLN) allocated to them,
- 4. that qualify as an agricultural and forestry holding to be registered in the Agricultural and Forestry Holding Information System (LFBIS) pursuant to § 1 para 1 of the Agricultural and Forestry Holding Information System Act, Federal Law Gazette No. 448/1980, and that do not fall under subparas 1 to 3 shall be the GLN allocated to them,
  - 5. that have initiated an electronic procedure to set up a business within the meaning of § 3 subpara 20 of the Federal Statistics Act 2000 and that do not fall under subparas 1 to 4 shall be the GLN allocated to them,
  - 6. entered in the Supplementary Register for Other Data Subjects (para 4) shall be the registration number allocated in the Supplementary Register.

(3a) The GLN is uniquely allocated to each data subject for the entire duration of his existence as a data subject within the meaning of para 3 subparas 3 to 5. It is allocated on behalf of the federal fiscal authorities in the case of para 3 subpara 3, on behalf of the Federal Minister in charge of agriculture, regions and tourism in the case of para 3 subpara 4 and on behalf of the operator of the Business Service Portal in the case of para 3 subpara 5, in each case by Statistics Austria upon registration in the business register pursuant to § 25 of the Federal Statistics Act 2000. If the reason for registration is replaced by a different reason pursuant to para 3 subparas 3 to 5, the allocated GLN shall remain valid as an identifier of the relevant data subject and no new GLN shall be allocated. If a data subject within the meaning of para 3 subpara 1 or subparas 3 to 6 is a natural person, the Register of Company Names number, GLN or registration number shall be used only insofar as that person's identity as a sole trader entered in the Register of Company Names, as a business pursuant to § 3 subpara 20 of the Federal Statistics Act 2000, as an agricultural and forestry holding, as a natural person in the context of an electronic procedure initiated to set up a business within the meaning of § 3 subpara 20 of the Federal Statistics Act 2000 or as other data subject is concerned.

Unternehmens im Sinne des § 3 Z 20 Bundesstatistikgesetz 2000 oder seine Eigenschaft als sonstiger Betroffener betroffen ist.

(4) Das Ergänzungsregister wird getrennt nach natürlichen Personen und sonstigen Betroffenen geführt. Unbeschadet des Abs. 3 sind im Ergänzungsregister für natürliche Personen auf Antrag des jeweiligen Betroffenen oder in den Fällen des § 10 Abs. 2 auf Antrag des Verantwortlichen der Datenverarbeitung natürliche Personen einzutragen, die nicht im Zentralen Melderegister eingetragen sind. In das Ergänzungsregister für sonstige Betroffene sind auf Antrag des jeweiligen Betroffenen oder in den Fällen des § 10 Abs. 2 auf Antrag des Verantwortlichen der Datenverarbeitung einzutragen:

1. Gebietskörperschaften und andere Körperschaften oder Anstalten des öffentlichen Rechts sowie
2. sonstige Betroffene, für die keine Stammzahl gemäß Abs. 3 Z 1 bis 5 zu bilden ist und sofern es sich bei diesen um natürliche Personen handelt nur im Hinblick auf ihre Eigenschaft als sonstiger Betroffener (§ 2 Z 7).

Voraussetzung für die Eintragung ist der Nachweis der Daten, die in Abs. 7 und der gemäß Abs. 7 zu erlassenden Verordnung des Bundesministers für Digitalisierung und Wirtschaftsstandort festgelegt sind. Zu den sonstigen Betroffenen können Handlungsvollmachten eingetragen werden.

*(Anm.: Abs. 4a bis 4c aufgehoben durch BGBl. I Nr. 119/2022)*

(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 ein E-ID für Zwecke der eindeutigen Identifikation im Sinne dieses Bundesgesetzes verwendet werden. Bei Verantwortlichen des privaten Bereichs gilt dies nur dann, wenn diese die Verwendung solcher Identifizierungsmittel zulassen. 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 für natürliche Personen 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

(4) The Supplementary Register shall be divided into sections for natural persons and for other data subjects. Without prejudice to para 3, natural persons who are not entered in the Central Register of Residents shall be entered in the Supplementary Register for Natural Persons upon application by the relevant data subject or, in the cases of § 10 para 2, upon application by the controller of the data processing system. The following shall be entered in the Supplementary Register for Other Data Subjects upon application by the relevant data subject or, in the cases of § 10 para 2, upon application by the controller of the data processing system:

1. territorial authorities and other corporations or institutions under public law, and
2. other data subjects for whom no source PIN must be generated pursuant to para 3 subparas 1 to 5; insofar as these data subjects are natural persons, they shall be entered only with regard to their capacity as other data subject (§ 2 subpara 7)

Registration shall be conditional on proof of the data specified in para 7 and in the regulation of the Federal Minister of Digital and Economic Affairs to be adopted pursuant to para 7. It is possible to enter commercial powers of attorney with regard to other data subjects.

*(Note: paras 4a to 4c repealed by Federal Law Gazette I No. 119/2022)*

(5) Electronic identification means of another Member State of the European Union that meet the requirements of Art. 6 para 1 of the eIDAS Regulation can be used in dealings with public-sector controllers in the same way as an eID for the purposes of unique identification as defined in this Federal Act. In the case of private-sector controllers, this only applies if such controllers allow the use of such identification means. 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 Natural Persons. 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

die Personenidentifikationsdaten des verwendeten elektronischen Identifizierungsmittels in das entsprechende Register einzutragen. Bei der eindeutigen Identifikation im elektronischen Verkehr ist die Personenbindung sinngemäß nach § 4 Abs. 5 oder § 14 Abs. 3 zu erstellen.

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

(7) Der Bundesminister für Digitalisierung und Wirtschaftsstandort kann im Einvernehmen mit dem Bundesminister für Inneres sowie dem Bundesminister für Finanzen mit Verordnung soweit erforderlich nähere Regelungen zum Ergänzungsregister, insbesondere zu den Eintragungsdaten (Namen oder Bezeichnung, Geburtsdatum, Geburtsort, Geschlecht, akademische Grade, Daten der vorgelegten amtlichen Dokumente, Telefonnummer, E-Mail-Adresse, Adresse, Anschrift, Sitz, Staatsangehörigkeit, Angaben über die Rechts- oder Organisationsform und Angaben über den Bestandszeitraum von Betroffenen) und bei welchen Stellen der Nachweis von personenbezogenen Daten für die Eintragung in das Ergänzungsregister erbracht werden kann, erlassen. In dieser Verordnung kann weiters geregelt werden, inwieweit ein Kostenersatz für die Eintragung zu leisten ist.

#### **Ergänzungsregister für natürliche Personen**

**§ 6a.** (1) Verantwortliche des öffentlichen Bereichs, deren Datenverarbeitung gemäß § 10 Abs. 2 mit bPK ausgestattet wurde, haben die ihnen zur Kenntnis gelangten Änderungen der Eintragungsdaten des Ergänzungsregisters für natürliche Personen (ERnP) sowie das Sterbedatum von betroffenen Personen dem Verantwortlichen im Wege des Auftragsverarbeiters, dessen sich die Stammzahlenregisterbehörde gemäß § 7 Abs. 2 bedient, nach Maßgabe der vorhandenen technischen Möglichkeiten zu melden. Der Auftragsverarbeiter hat die Änderung im Auftrag des Verantwortlichen vorzunehmen.

(2) Zum Zwecke der Aktualisierung ist die Stammzahlenregisterbehörde auf Verlangen von Verantwortlichen des öffentlichen Bereichs ermächtigt, diesen laufend in geeigneter elektronischer Form die geänderten Eintragungsdaten des ERnP, in Bezug auf Personen, für die ein bPK aus dem Bereich gespeichert ist, in dem der jeweilige Verantwortliche zur Vollziehung berufen ist, zu übermitteln.

identification means used must be entered in the relevant register. In the case of unique identification in electronic communications, the identity link shall be created pursuant to § 4 para 5 or § 14 para 3 applied mutatis mutandis.

(6) For the generation of source PIN for natural persons, mathematical algorithms which apply strong cryptography to the CRR number or the registration number of the Supplementary Register for Natural Persons must be used in the source PIN register. These algorithms shall be determined by the Source PIN Register Authority and – with the exception of the cryptographic keys used – published on the Internet.

(7) With the consent of the Federal Minister of the Interior and the Federal Minister of Finance, the Federal Minister of Digital and Economic Affairs may, where necessary, lay down, by regulation, detailed provisions governing the Supplementary Register, in particular as regards the registration data (name or designation, date of birth, place of birth, sex, academic degrees, data of the official documents submitted, telephone number, email address, address, postal address, registered office, nationality, details of the legal or organisational form and details of the period of existence of a data subject) and the bodies to which proof of personal data required for registration in the Supplementary Register may be submitted. Moreover, this regulation may also specify to what extent the costs of registration must be reimbursed.

#### **Supplementary Register for Natural Persons**

**§ 6a.** (1) In accordance with the existing technical possibilities, public-sector controllers whose data processing systems include sector-specific personal identifiers pursuant to § 10 para 2 shall report to the controller, through the processor to which the Source PIN Register Authority has recourse pursuant to § 7 para 2, any changes to the registration data entered in the Supplementary Register for Natural Persons (SRNP) of which they have obtained knowledge as well as the date of death of the persons concerned. The processor shall implement the change on behalf of the controller.

(2) For the purpose of updating information, the Source PIN Register Authority is authorised, at the request of public-sector controllers, to regularly send them, by appropriate electronic means, any changed registration data of the SRNP with regard to persons for whom a sector-specific personal identifier from the sector in which the relevant controller has been entrusted with implementation duties is stored.

(3) Der Auftragsverarbeiter im Sinne des Abs. 1 hat im Auftrag des Verantwortlichen mittels eines Abgleichs zwischen dem ZMR und ErnP datenqualitätssichernde Maßnahmen, insbesondere im Hinblick auf eine mögliche Identität ähnlicher Datensätze in diesem Ergänzungsregister, auf bereits vorhandene Eintragungen im ZMR oder auf die Schreibweisen von Namen und Adressen, zu setzen

#### **Ergänzungsregister für sonstige Betroffene**

§ 6b. (1) Das Ergänzungsregister für sonstige Betroffene (ERsB) dient dem Nachweis der eindeutigen Identität Betroffener im Sinne des § 2 Z 7 und dokumentiert bereits bestehende Vollmachtsverhältnisse in elektronischer Form. Eintragungen ins ErsB haben keine konstitutive Wirkung.

(2) Die Führung des ERsB ist Aufgabe der Stammzahlenregisterbehörde. Die Eintragung in das Register erfolgt durch die Stammzahlenregisterbehörde oder durch eine Institution, die unmittelbar durch Gesetz, Verordnung oder völkerrechtlichen Vertrag eingerichtet ist oder der dadurch Rechtspersönlichkeit zuerkannt wurde, für

1. sich,
2. ihre Teilorganisationen,
3. die ihrer gesetzlichen Aufsicht unterliegenden Organisationen,
4. Betroffene, soweit die Institution durch Gesetz oder Verordnung dazu ermächtigt wurde.

Die Stammzahlenregisterbehörde und die in dieser Bestimmung genannten Institutionen sind als gemeinsam Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 Abs. 1 DSGVO ermächtigt, die personenbezogenen Daten im ERsB gemeinsam in der Art zu verarbeiten, dass jeder Verantwortliche auch auf jene Daten Zugriff hat, die von den anderen Verantwortlichen zur Verfügung gestellt wurden. Die Erfüllung von Informations-, Auskunfts-, Berichtigungs-, Löschungs- und sonstigen Pflichten nach den Bestimmungen der DSGVO gegenüber dem Betroffenen obliegt der Stammzahlenregisterbehörde.

(3) Das ERsB ist in Bezug auf Betroffene, die keine natürlichen Personen sind und ausschließlich in Bezug auf die Vor- und Nachnamen ihrer vertretungsbefugten natürlichen Personen hinsichtlich des aktuellen Datenbestands als öffentliches Register zu führen, das von der Stammzahlenregisterbehörde im Internet verfügbar gehalten wird.

(3) The processor within the meaning of para 1 shall, on behalf of the controller, take measures to assure data quality by reconciling the data contained in the CRR and the SRNP, in particular as regards any potential identity of similar sets of data contained in that Supplementary Register, any data already registered in the CRR or the spelling of names and addresses.

#### **Supplementary Register for Other Data Subjects**

§ 6b. (1) The Supplementary Register for Other Data Subjects (SRODS) serves to validate the unique identity of data subjects within the meaning of § 2 subpara 7 and documents existing powers of attorney in electronic form. Registration in the SRODS does not create or alter rights.

(2) The Source PIN Register Authority is responsible for keeping the SRODS. Entries in the register are made by the Source PIN Register Authority or by any institution directly established, or vested with legal personality, by law, regulation or international agreement

1. on its own behalf,
2. on behalf of its sub-organisations,
3. on behalf of the organisations subject to its legal supervision,
4. on behalf of data subjects, insofar as the institution is authorised to do so by law or regulation.

The Source PIN Register Authority and the institutions referred to in this provision shall be authorised, as joint controllers pursuant to Art. 4 subpara 7 in connection with Art. 26 para 1 of the GDPR, to jointly process the personal data contained in the SRODS in such a way that each controller also has access to the data provided by the other controllers. The Source PIN Register Authority is responsible for ensuring compliance with the obligations in connection with information, access, rectification, erasure and other rights of data subjects under the GDPR.

(3) With regard to the data currently recorded in the register in relation to data subjects who are not natural persons and, as far as any natural persons authorised to represent such data subjects are concerned, only with regard to their first and last names, the SRODS shall be kept as a public register that is made available on the Internet by the Source PIN Register Authority.

(4) Die Stammzahlenregisterbehörde hat Eintragungen, zu denen ihr Änderungen bekannt werden, richtig zu stellen oder inaktiv zu setzen. Ersetzte oder inaktive Eintragungen sind unverzüglich zu löschen, sobald diese für die in diesem Bundesgesetz angeführten Zwecke nicht mehr benötigt werden, spätestens jedoch nach Ablauf von dreißig Jahren.

(5) Die Stammzahlenregisterbehörde hat auf Verlangen jeder Person einen mit einer Amtssignatur (§ 19 E-GovG) versehenen Auszug der aktuellen Daten aus dem Register elektronisch auszustellen. Dazu hat die Stammzahlenregisterbehörde ein Webformular und soweit zweckmäßig eine Schnittstelle zur Verfügung zu stellen. Bei Registerabfragen und auf Auszügen aus dem Register ist die Eintragungsstelle klar ersichtlich zu machen und ein Hinweis aufzunehmen, dass der Eintrag im ERsB nicht konstitutiv ist.

#### **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 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

(4) If the Source PIN Register Authority becomes aware of any changes to entries, it shall rectify such entries or set the status of such entries to inactive. Replaced or inactive entries shall be deleted immediately as soon as they are no longer needed for the purposes specified in this Federal Act, but no later than after a period of thirty years.

(5) The Source PIN Register Authority shall, at the request of any person, issue an electronic excerpt of current data from the register bearing an official signature (§ 19 of the [E-Government Act](#)). The Source PIN Register Authority shall provide an online form and, if appropriate, an interface for this purpose. Data retrievals from the register and register excerpts must clearly indicate the registering entity and contain reference to the fact that registration in the SRODS does not create or alter rights.

#### **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 PIN and conducting the procedures governed by § 4, § 4b, § 5, § 9, § 10, § 14, § 14a and § 15, the Source PIN Register Authority may have recourse 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

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.

(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

respect to data subjects who are not natural persons, the source PIN 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 PIN 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) The mathematical algorithms applied to generate the sector-specific personal identifier (hash function using the source PIN and 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 PIN 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 para 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

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.

#### **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.

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 para 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 para 2 shall also be governed by the regulation to be adopted pursuant to § 4 para 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.

#### **Protection of the source PIN of natural persons**

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

1. The source PIN of natural persons may be permanently stored only in encrypted form.
2. The processing of the source PIN of natural persons in order to generate the sector-specific personal identifier must not give rise to any storage of the source PIN 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 para 8.

(2) The source PIN 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 para 5, § 14 para 3 and § 14a para 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 para 2 and § 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

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 DSGVO) kann durch Einsatz des E-ID ein bPK gebildet werden, wobei anstelle

### **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 PIN. 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 para 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. 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 (para 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 para 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 para 4 of the [Data Protection Act](#)), a sector-specific personal identifier may be derived using the eID, wherein the

der Bereichskennung die Stammzahl oder das bPK des Verantwortlichen des privaten Bereichs tritt. Voraussetzung hierfür ist, dass der Verantwortliche des privaten Bereichs eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet hat, in der seine Stammzahl oder sein bPK 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 oder ihrem eigenen bPK als Bereichskennung gebildet wurden.

(3) Verwendet der E-ID-Inhaber den 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 zum E-ID-Inhaber enthält, zu erstellen, und an die betreffende Datenverarbeitung zu übermitteln. Wird die Erstellung der Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers ausgelöst (§ 2 Z 10a erster Fall), hat der qualifizierte VDA die verschlüsselte Stammzahl und die zugehörigen Sicherheitsdaten der Stammzahlenregisterbehörde zur Verfügung zu stellen. Mit Einwilligung des E-ID-Inhabers können in die Personenbindung Vorname, Familienname oder Geburtsdatum, sowie nach Maßgabe der technischen Möglichkeiten weitere Merkmale zu diesem aus für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen oder privaten 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 staatspezifisches Kennzeichen oder bei Anwendungen internationaler Organisationen ein organisationsspezifisches Kennzeichen zu verwenden ist.

(2) Verwendet der E-ID-Inhaber den 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. Wird die Erstellung der Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers ausgelöst (§ 2 Z 10a erster Fall), hat der qualifizierte VDA die verschlüsselte Stammzahl und die zugehörigen Sicherheitsdaten der Stammzahlenregisterbehörde zur Verfügung zu stellen. Nach Maßgabe der technischen Möglichkeiten können mit Einwilligung des E-ID-

source PIN or sector-specific personal identifier 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 or sector-specific personal identifier 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 PIN or sector-specific personal identifier as sector code.

(3) If the eID holder uses the eID in electronic communications pursuant to para 1, the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (§ 4 para 2) containing a sector-specific personal identifier relating to the eID holder and send it to the relevant data processing system. If the creation of the identity link is triggered by means of a qualified electronic signature of the eID holder (§ 2 subpara 10a first case), the qualified TSP shall provide to the Source PIN Register Authority the encrypted source PIN and the associated security data. With the consent of the eID holder, 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 or private-sector controllers which the Source PIN Register Authority can access can be included in the identity link. § 4 para 6 shall apply mutatis mutandis.

#### **eID-compatible applications abroad**

**§ 14a.** (1) For eID-compatible applications abroad § 14 para 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) If the eID holder uses the eID in electronic communications pursuant to para 1, the Source PIN Register Authority or an authority acting on its behalf shall create an identity link (§ 4 para 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. If the creation of the identity link is triggered by means of a qualified electronic signature of the eID holder (§ 2 subpara 10a first case), the qualified TSP shall provide to the Source PIN Register Authority the encrypted source PIN and the associated security data. In accordance with the technical possibilities, further data of the eID holder taken from registers of public-

Inhabers in die Personenbindung weitere Merkmale zu diesem aus für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen oder privaten 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 DSGVO 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 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.

### **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 hierfür 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

sector or private-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 PIN 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 controllers have to establish the unique identity of their customers because of statutory provisions or provide a technical environment corresponding to § 14 para 1 second sentence to their clients and
2. personal data will be processed 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 para 2) like a public-sector controller.

(2) The Federal Minister of the Interior is authorised to determine, by regulation, a reimbursement of costs incurred by the generation of sector-specific personal identifiers and encrypted sector-specific personal identifiers pursuant to para 1.

### **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 para 2 of the Federal Fiscal Code.

(2) Where validation of the personal data referred to in para 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

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 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.

*(Anm.: Z 2 aufgehoben durch BGBl. I Nr. 117/2024)*

#### **über personenbezogene Daten aus elektronischen Registern eines Verantwortlichen des öffentlichen oder privaten Bereichs**

§ 18. (1) Personenbezogene Daten, die gemäß § 4b Abs. 1 Z 1 bis 5 und 8 oder in einem für die Stammzahlenregisterbehörde zugänglichen elektronischen Register eines Verantwortlichen des öffentlichen oder privaten Bereichs enthalten sind, sind

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 in accordance with the technical possibilities undertake the acquisition of the data via electronic communications to the extent this is necessary, provided that the data subject has consented to such acquisition 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 para 4 of the Registration Act.

(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 para 1.

*(Note: subpara 2 repealed by Federal Law Gazette I No. 117/2024)*

#### **regarding personal data from electronic registers of a public-sector or private-sector controller**

§ 18. (1) When the eID function is used, personal data contained pursuant to § 4b para 1 subparas 1 to 5 and 8 or in an electronic register of a public-sector or

bei der Verwendung der Funktion E-ID nach Maßgabe der technischen Möglichkeiten

1. dem E-ID-Inhaber selbst,
2. Verantwortlichen des öffentlichen Bereichs im Auftrag des E-ID-Inhabers für Verfahren für die diese eine für den Einsatz des E-ID taugliche technische Umgebung eingerichtet haben, oder
3. Dritten im Auftrag des E-ID-Inhabers, sofern ihnen die Nutzung des E-ID-Systems eröffnet und noch nicht unterbunden wurde,

zu übermitteln. Es ist sicherzustellen, dass die Protokollierung der Datenübermittlung aus dem E-ID-System im Auftrag des E-ID-Inhabers unbeschadet der datenschutzrechtlichen Verpflichtungen des Verantwortlichen und seiner Auftragsverarbeiter nur dem E-ID-Inhaber zugänglich ist.

(2) Der Bundesminister für Inneres ist ermächtigt, Dritten gemäß Abs. 1 Z 3 die Nutzung des E-ID-Systems zu eröffnen. Dritte gemäß Abs. 1 Z 3 haben sich hierfür beim Bundesminister für Inneres zu registrieren. 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. Dritte haben dem Bundesminister für Inneres jeden Umstand bekanntzugeben, der einer Nutzung entgegensteht. Der Bundesminister für Inneres ist zum Zwecke der Eröffnung der Nutzung des E-ID-Systems berechtigt, im Datenfernverkehr

1. Informationen über nicht getilgte rechtskräftige strafgerichtliche Verurteilungen (§ 9 Abs. 1 Z 1 des Strafregistergesetzes 1968, BGBl. Nr. 277/1968) von Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes (VStG), BGBl. Nr. 52/1991, insbesondere wegen widerrechtlichen Zugriffes auf ein Computersystem (§ 118a des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974), Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) oder wegen des missbräuchlichen Abfangens von Daten (§ 119a StGB), sowie
2. die genaue Bezeichnung des Gewerbes (§ 365a Abs. 1 Z 5 der Gewerbeordnung 1994 (GewO 1994), BGBl. Nr. 194/1994, aus dem Gewerbeinformationssystem Austria (GISA) gemäß § 365 GewO 1994 mithilfe der GISA-Zahl

abzufragen. Die gemäß Abs. 1 übermittelten personenbezogenen Daten dürfen im konkreten Fall nur für die glaubhaft gemachten eigenen Zwecke verarbeitet werden;

private-sector controller which the Source PIN Register Authority can access must be transferred, in accordance with the technical possibilities,

1. to the eID holder,
2. to public-sector controllers on behalf of the eID holder for procedures for which such controllers have set up a technical environment in which the eID can be used, or
3. 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.

It must be ensured that, without prejudice to the obligations of the controller and the controller's processors under data protection law, solely the eID holder has access to records relating to the transfer of data from the eID system effected on behalf of the eID holder.

(2) The Federal Minister of the Interior is authorised to allow third parties as referred to in para 1 subpara 3 to use the eID system. For this purpose, third parties as referred to in para 1 subpara 3 must register with the Federal Minister of the Interior. They must not be allowed to use the eID system 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. Third parties shall notify the Federal Minister of the Interior of any circumstances that preclude the use of the eID system. For the purpose of allowing use of the eID system, the Federal Minister of the Interior is entitled to retrieve, via electronic communications,

1. information on unspent final criminal convictions (§ 9 para 1 subpara 1 of the Criminal Records Act 1968, Federal Law Gazette No. 277/1968) of persons responsible pursuant to § 9 of the Administrative Penal Act, Federal Law Gazette No. 52/1991, in particular for illegal access to a computer system (§ 118a of the Criminal Code, Federal Law Gazette No. 60/1974), breach of telecommunication confidentiality (§ 119 of the Criminal Code) or improper interception of data (§ 119a of the Criminal Code), and
2. the exact designation of the trade (§ 365a para 1 subpara 5 of the Trade, Commerce and Industry Regulation Act 1994, Federal Law Gazette No. 194/1994) from the Austrian Business Licence Information System (GISA) pursuant to § 365 of the Trade, Commerce and Industry Regulation Act 1994 by means of the GISA number.

The personal data transferred pursuant to para 1 may, in a specific case, be processed only for the third party's own purposes that have been credibly demonstrated; the

die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck im Sinne dieser Bestimmung.

(3) Der Bundesminister für Inneres ist im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort ermächtigt, nähere Bestimmungen über die Vorgangsweise gemäß Abs. 1 und 2 durch Verordnung festzulegen, insbesondere inwieweit neben Unternehmern und Vereinen auch andere Teilnehmer des Unternehmensserviceportals gemäß § 5 des Unternehmensserviceportalgesetzes (USPG), BGBl. I Nr. 52/2009, oder andere Dritte registriert werden können und inwieweit Dritte gemäß Abs. 1 Z 3 sowohl die Kosten für die Eröffnung der Nutzung als auch für die Nutzung des E-ID-Systems zu ersetzen haben.

(4) Die Rechtmäßigkeit der Zugänglichkeit elektronischer Register eines Verantwortlichen des öffentlichen Bereichs für die Stammzahlenregisterbehörde im Sinne des Abs. 1 ist auf Grund einer Rechtsgrundlage in einem Materiangesetz zu beurteilen. Der für die jeweilige Datenverarbeitung zuständige Bundesminister kann im Rahmen einer gesetzlichen Ermächtigung zur Datenverarbeitung, die für eine Übermittlung gemäß Abs. 1 in Betracht kommenden Identitätsdaten, Informationen zu Berechtigungen sowie Umstände, die der Betroffene nachweisen möchte, mit Verordnung näher konkretisieren.

(5) Sofern es sich bei Dritten gemäß Abs. 1 Z 3 um Unternehmer im Sinne des § 1 des Unternehmensgesetzbuches (UGB), dRGBL. S 2019/1897, oder um Vereine im Sinne des § 1 des Vereinsgesetzes 2002 (VerG), BGBl. I Nr. 66/2002, handelt, haben diese im Zuge der Antragstellung jedenfalls

1. den Namen und die Rechtsform im Sinne des § 25 Abs. 1 Z 1 des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999,
2. die Verantwortlichen gemäß § 9 VStG,
3. die Daten gemäß § 25 Abs. 1 Z 2 und 3 des Bundesstatistikgesetzes 2000,
4. gegebenenfalls die GISA-Zahl, die Firmenbuchnummer, die ZVR-Zahl und das Logo,
5. den Unternehmensgegenstand oder Vereinszweck,
6. die Telefonnummer und eine E-Mail-Adresse des Unternehmens oder des Vereins sowie

mere transfer of personal data obtained through the use of the eID to others is not considered an own purpose within the meaning of this provision.

(3) The Federal Minister of the Interior, with the consent of the Federal Minister of Digital and Economic Affairs, is authorised to specify, by regulation, detailed provisions on the procedure pursuant to paras 1 and 2, in particular on the extent to which participants of the Business Service Portal pursuant to § 5 of the Business Service Portal Act, Federal Law Gazette I No. 52/2009, other than entrepreneurs and associations, or other third parties can be registered or the extent to which third parties as referred to in para 1 subpara 3 are required to reimburse the costs of establishing access to and using the eID system.

(4) The Source PIN Register Authority can lawfully access electronic registers of a public-sector controller within the meaning of para 1 if such access has a legal basis in subject-specific legislation. The Federal Minister in charge of the relevant data processing system may, on the basis of a legal authorisation for data processing, issue a regulation to specify, in more concrete terms, the identity data, details of authorisations and circumstances to be established by a data subject that may be transferred pursuant to para 1.

(5) If a third party as referred to in para 1 subpara 3 is an entrepreneur within the meaning of § 1 of the Business Code, German Imperial Law Gazette p. 2019/1897, or an association within the meaning of § 1 of the Associations Act 2002, Federal Law Gazette I No. 66/2002, such entrepreneur or association shall, when filing an application for the use of the eID system, at the very least provide

1. the name and the legal form within the meaning of § 25 para 1 subpara 1 of the Federal Statistics Act 2000, Federal Law Gazette I No. 163/1999,
2. the persons responsible pursuant to § 9 of the Administrative Penal Act,
3. the information pursuant to § 25 para 1 subparas 2 and 3 of the Federal Statistics Act 2000,
4. if applicable, the GISA number, the Register of Company Names number, the ZVR number and the logo,
5. the object of the business or the purpose of the association,
6. the telephone number and an email address of the business or association, and

7. die für die Nutzung des E-ID-Systems glaubhaft gemachten Zwecke anzugeben, sofern diese Daten nicht bereits im Wege des Unternehmensregisters gemäß § 25 des Bundesstatistikgesetzes 2000 ermittelt werden können. Darüber hinaus kann der Unternehmer oder der Verein den akademischen Grad, die Vor- und Familiennamen, die Telefonnummer und E-Mail-Adresse einer oder mehrerer Kontaktpersonen angeben.

(6) Der Dritte gemäß Abs. 1 Z 3 hat eine Änderung der im Zuge der Registrierung angegebenen Informationen dem Bundesminister für Inneres unverzüglich bekanntzugeben. Teilnehmer des Unternehmensserviceportals gemäß § 5 USPG haben diese Änderungen im Wege des Unternehmensserviceportals bekanntzugeben. Wird das E-ID-System über einen Zeitraum von fünf Jahren nicht genutzt, sind sämtliche Daten des Dritten zu löschen.

(7) Sofern Dritten gemäß Abs. 1 Z 3 die Nutzung des E-ID-Systems eröffnet wurde, haben diese dem Bundesminister für Inneres unverzüglich zu melden, wenn:

1. sich ein glaubhaft gemachter Zweck gemäß Abs. 2 oder der Verantwortliche gemäß § 9 VStG ändert oder
2. Dritte die glaubhaft gemachten Zwecke gemäß Abs. 2 nicht mehr verfolgen wollen oder dürfen.

## **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

7. the credibly demonstrated purposes of the use of the eID system, unless such data can already be obtained from the business register pursuant to § 25 of the Federal Statistics Act 2000. In addition, the entrepreneur or association can provide the academic degree, first and family names, telephone number and email address of one or more contact persons.

(6) A third party as referred to in para 1 subpara 3 shall notify the Federal Minister of the Interior immediately of any changes to the information provided during registration. Participants of the Business Service Portal pursuant to § 5 of the Business Service Portal Act shall report such changes by means of the Business Service Portal. If the eID system is not used over a period of five years, all data relating to the third party shall be deleted.

(7) If a third party as referred to in para 1 subpara 3 has been allowed to use the eID system, such third party shall notify the Federal Minister of the Interior immediately if

1. a credibly demonstrated purpose pursuant to para 2 or the person responsible pursuant to § 9 of the Administrative Penal Act has changed, or
2. the third party no longer wishes or is no longer allowed to pursue the credibly demonstrated purposes pursuant to para 2.

## **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 para 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

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, RGBI. 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.

#### **Ersetzendes Scannen**

§ 20a. Die Behörde kann Anbringen und andere das Verfahren betreffende Unterlagen sowie Akten, die nicht gemäß § 21 Abs. 1 elektronisch erzeugt und genehmigt wurden, in ein elektronisches Dokument übertragen, sofern dies aufgrund von Art und Inhalt des ursprünglichen Originals tunlich erscheint. Ein auf diese Weise erzeugtes elektronisches Dokument kann das ursprüngliche Original mit derselben Beweiskraft ersetzen und gilt selbst als Original, sofern nach dem Stand der Technik die inhaltliche und bildliche Identität des Originals und des elektronischen Dokuments sowie die Unveränderbarkeit und Aufwärtskompatibilität des elektronischen Dokuments sichergestellt ist. Der Zeitpunkt der Übertragung ist unveränderbar zu dokumentieren.

#### **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.

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.

#### **Substitute Scanning**

§ 20a. The authority may convert submissions and other documents pertaining to the procedure as well as records that were not generated and approved electronically pursuant to § 21 para 1 into an electronic document if this appears feasible considering the nature and content of the original. An electronic document generated in this manner may substitute the original with the same probative value and is deemed as an original itself, provided that the original and the electronic document are identical in content and appearance and the electronic document is immutable and forward compatible according to the state of the art. The time of the conversion must be documented in an immutable manner.

#### **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) 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.

## **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.

## **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) 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.

## **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.

## **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 PIN 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 a sector-specific personal identifier of another private-sector controller without authorisation; or

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.

## **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 alle Geschlechter 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

3. makes available to other private-sector controllers the sector-specific personal identifiers derived from his own source PIN 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 para 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 para 1 may be imposed.

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

## **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 all genders.

#### **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 para 3, § 2 subparas 8 and 10, § 3 para 1, § 5, § 6 paras 2 to 6, § 7 para 2, § 8, the heading before § 9, § 9 paras 1 and 2, the heading before § 10, § 10 paras 1 to 3, the heading before § 11, § 11, § 12 para 1 subpara 4 and para 2, the heading before § 13, § 13 paras 1 to 3, the heading before § 14, § 14 paras 1 and 2, the heading before § 15, § 15 paras 1 and 2, § 19 paras 1 to 3, § 20, the heading before § 22, § 22 para 1 subparas 1 to 4 and § 25 paras 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 subpara 3 shall expire.

(3) The table of contents, the heading of § 17 and § 17 para 2 as amended by the Budget Accompanying Act 2011, Federal Law Gazette I No. 111/2010, shall

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.

(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 <sup>(Anm. 1)</sup>.

(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 *(Anm.: offensichtlich gemeint: 5a. 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 <sup>(Anm. 2)</sup>.

(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,

enter into force on 1 January 2011. Authorities shall apply § 17 para 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 subparas 1, 4, 10 and 11, § 2a, § 4 para 2, § 6 paras 4 and 6, § 7 para 1, § 8, the headings before § 9, § 10 para 2, the heading of Part III, § 14 para 1, § 14a, § 16 para 2, § 17 para 2 and para 3 subpara 2, § 19 paras 1 and 3, § 22 paras 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 subpara 6 and § 25 with heading shall expire.

(5) The table of contents, the heading of Part II, § 2 subpara 11, § 4 para 5, § 6 para 2, § 10 para 2 last sentence and para 3, § 13 para 2 first sentence, § 15 paras 1, 1a and 2 last sentence, the heading of § 17, § 17 para 2 last sentence, § 21 para 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 promulgation of 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 para 8 of the [Service of Documents Act \(Note 1\)](#).

(6) The table of contents, the heading of Part II, § 2 subpara 10, § 4, § 4a, § 4b and § 5 including the headings, § 6 paras 1, 4 and 5, § 7 para 2, § 8 first sentence, § 10 including the heading, § 12, the heading of Part III, § 14 paras 1 and 3, § 14a including the heading, § 15, § 18 including the heading, Part V *(Note: should obviously read Part Va)*, § 25 paras 2 and 3 and § 28 subparas 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 paras 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 <sup>(Note 2)</sup>.

(7) The entries in the table of contents regarding § 8, § 14, § 15 to § 18 and § 22, § 3, § 4 paras 1, 2, 4, 5 and 6, § 4a paras 3 to 5, § 4b, § 5 paras 1 to 3, § 6 paras 2 and 4, § 7 para 2, § 8 including the heading, § 9 paras 1 and 2, § 10 paras 1 and 2, § 11, § 12, § 13, § 14 including the heading, § 14a para 2, the heading of § 15, § 15 para 1, the heading of § 16, § 16 para 2, § 17 including the heading, the heading

§ 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 Bundesminister 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 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.

(9) Der Eintrag im Inhaltsverzeichnis zu § 18, § 1b Abs. 1, § 2 Z 10a, § 4 Abs. 4 bis 6, § 4a Abs. 3 und 4, § 4b Abs. 1 Z 1 und 8, Abs. 2 bis 5, § 6 Abs. 1 und Abs. 4 bis 4c, § 14, § 14a Abs. 2, § 18 samt Überschrift, § 23, § 25 Abs. 2 und § 28 Z 4 in der Fassung des Bundesgesetzes BGBl. I Nr. 169/2020 treten mit Ablauf des Tages der Kundmachung in Kraft und finden mit Ausnahme von § 1b Abs. 1 und § 25 Abs. 2 erst ab dem Zeitpunkt Anwendung, den der Bundesminister für Inneres gemäß Abs. 6 letzter Satz im Bundesgesetzblatt kundmacht.

(10) Der Eintrag im Inhaltsverzeichnis zu § 6b, § 6 Abs. 3, 3a, 4, 6 und 7, § 6b samt Überschrift und § 25 Abs. 4 in der Fassung des Bundesgesetzes BGBl. I Nr. 119/2022 treten ein Jahr nach dem Tag der Kundmachung in Kraft. Der Eintrag im Inhaltsverzeichnis zu § 6a, § 6 Abs. 4a bis 4c und § 6a samt Überschrift in der Fassung des Bundesgesetzes BGBl. I Nr. 119/2022 treten mit Ablauf des Tages der

of § 18, § 18 paras 1 and 2, § 19 paras 2 and 3, the heading of § 22, § 22 para 1, § 24 para 3 as well as § 25 para 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 para 2, § 9 paras 1 and 2, § 11, § 13, the heading of § 16, § 16 para 2, § 17 including the heading, § 19 paras 2 and 3, the heading of § 22, § 22 para 1, § 24 para 3 and § 25 para 2, shall apply only from the date which the Federal Minister of the Interior announces in the Federal Law Gazette pursuant to para 6 last sentence. § 6 para 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 para 6 last sentence.

(8) § 4 para 8, § 4a para 6, § 5 para 1, § 6 para 4, § 7, § 9 paras 1 and 2, § 10 para 2, the heading of § 14, the heading of § 15 as well as § 15 para 1 subpara 2, § 18 para 3, § 19 para 2, § 25 para 3 and § 28 subparas 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 para 1, § 9 paras 1 and 2, § 19 para 2, § 25 para 3 and § 28 subparas 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 para 6 last sentence. § 6 para 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 para 6. § 1 para 3 shall expire at the end of 22 September 2020.

(9) The entry in the table of contents regarding § 18, § 1b para 1, § 2 subpara 10a, § 4 paras 4 to 6, § 4a paras 3 and 4, § 4b para 1 subparas 1 and 8, paras 2 to 5, § 6 para 1 and para 4 to 4c, § 14, § 14a para 2, § 18 including the heading, § 23, § 25 para 2 and § 28 subpara 4 as amended by the federal act Federal Law Gazette I No. 169/2020 shall enter into force at the end of the date of promulgation and, with the exception of § 1b para 1 and § 25 para 2, shall apply only from the date which the Federal Minister of the Interior announces in the Federal Law Gazette pursuant to para 6 last sentence.

(10) The entry in the table of contents regarding § 6b, § 6 paras 3, 3a, 4, 6 and 7, § 6b including the heading and § 25 para 4 as amended by the federal act Federal Law Gazette I No. 119/2022 shall enter into force one year following the date of promulgation. The entry in the table of contents regarding § 6a, § 6 paras 4a to 4c and § 6a including the heading as amended by the federal act Federal Law Gazette I

Kundmachung in Kraft und finden erst ab dem Zeitpunkt Anwendung, den der Bundesminister für Inneres gemäß Abs. 6 letzter Satz im Bundesgesetzblatt kundmacht.

(11) Das Inhaltsverzeichnis, die Überschrift des § 1a, § 1a Abs. 3, § 1c samt Überschrift, § 4 Abs. 6, § 4a Abs. 3 und 4, § 14a Abs. 2, § 17 Abs. 3 Z 1, § 20a samt Überschrift und § 25 Abs. 5 und 6 in der Fassung des Bundesgesetzes BGBl. I Nr. 117/2024 treten mit Ablauf des Tages der Kundmachung des Bundesgesetzes BGBl. I Nr. 117/2024 in Kraft. Gleichzeitig tritt § 17 Abs. 3 Z 2 außer Kraft.

(\_\_\_\_\_)

*Anm. 1: vgl. BGBl. I Nr. 33/2018 vom 30.5.2018*

*Anm. 2: gemäß BGBl. II Nr. 340/2023: 5.12.2023)*

### **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. Die im Rahmen des Pilotbetriebs verarbeiteten Registrierungsdaten dürfen ab dem gemäß § 24 Abs. 6 festgelegten Zeitpunkt zum Zwecke der Verwaltung und Nutzung des E-ID gemäß § 4b Abs. 1 und § 18 Abs. 1 weiterverarbeitet werden. Die Verarbeitung dieser Daten zu anderen Zwecken ist nur auf Grund gesetzlicher Anordnung zulässig. Betroffene, die bereits vor dem gemäß § 24 Abs. 6 festgelegten Zeitpunkt im Rahmen eines Pilotbetriebs behördlich unter Anwendung des § 4a registriert wurden, dürfen ihren E-ID bis zum Ablauf der Gültigkeitsdauer weiterverwenden.

(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

No. 119/2022 shall enter into force at the end of the date of promulgation and shall apply only from the date which the Federal Minister of the Interior announces in the Federal Law Gazette pursuant to para 6 last sentence.

(11) The table of contents, the heading of § 1a, § 1a para 3, § 1c including the heading, § 4 para 6, § 4a paras 3 and 4, § 14a para 2, § 17 para 3 subpara 1, § 20a including the heading and § 25 paras 5 and 6 as amended by the federal act Federal Law Gazette I No. 117/2024 shall enter into force at the end of the date of promulgation of the federal act Federal Law Gazette I No. 117/2024. At the same time, § 17 para 3 subpara 2 shall expire.

(\_\_\_\_\_)

*Note 1: cf. Federal Law Gazette I No. 33/2018 of 30 May 2018*

*Note 2: pursuant to Federal Law Gazette II No. 340/2023, 5 December 2023)*

### **Transitional provisions**

**§ 25.** (1) The courts and administrative authorities established by federal legislation are obligated to create, by no later than 1 January 2020, the technical and organisational capacities for electronic communications with the involved parties pursuant to § 1a.

(2) Following promulgation of the federal act 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. The registration data processed in the context of such trial operations may be further processed from the date specified pursuant to § 24 para 6 for the purpose of the administration and use of the eID pursuant to § 4b para 1 and § 18 para 1. Processing these data for other purposes is permissible only on the basis of special instructions laid down by law. Data subjects who were registered by an authority before the date specified pursuant to § 24 para 6 in the context of a trial operation in accordance with § 4a may continue to use their eID until it expires.

(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 para 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

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.

(4) Die bis zum Inkrafttreten des BGBl. I Nr. 119/2022 für Betroffene im Sinne des § 6 Abs. 3 Z 3 bis 5 verwendete Ordnungsnummer des ERsB ist als GLN weiter zu verwenden. Die zu diesen Betroffenen im ERsB verarbeiteten Daten sind zu diesem Zeitpunkt im Auftrag des jeweiligen Verantwortlichen an die Bundesanstalt „Statistik Österreich“ für Zwecke der Eintragung in das Unternehmensregister gemäß § 6 Abs. 3 Z 3 bis 5 zu übermitteln und aus dem ERsB zu löschen.

(5) Verantwortliche des öffentlichen Bereichs, deren Einrichtung in Gesetzgebung Bundessache ist, sind bis längstens 31. Dezember 2025 von der Verpflichtung nach § 1c ausgenommen, soweit sie nicht über die für den elektronischen Verkehr erforderlichen technischen oder organisatorischen Voraussetzungen verfügen.

(6) Die Gerichte und Verwaltungsbehörden, deren Einrichtung in Gesetzgebung Bundessache ist, sind verpflichtet, bis spätestens 1. Jänner 2025 die technischen und organisatorischen Voraussetzungen für die Prüfung eines vereinfachten Nachweises gemäß § 4 Abs. 6 letzter Satz zu schaffen.

#### **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.

#### **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,

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.

(4) The registration number of the SRODS used for data subjects within the meaning of § 6 para 3 subparas 3 to 5 until the entry into force of Federal Law Gazette I No. 119/2022 shall continue to be used as GLN. The data processed in the SRODS in relation to such data subjects shall, at such time, be transferred to Statistics Austria on behalf of the relevant controller for the purpose of registration in the business register pursuant to § 6 para 3 subparas 3 to 5 and shall be deleted from the SRODS.

(5) Public-sector controllers established by federal legislation shall be exempted from the obligation pursuant to § 1c until no later than 31 December 2025 if they lack the technical or organisational capacities required for electronic communications.

(6) The courts and administrative authorities established by federal legislation are obligated to create, by no later than 1 January 2025, the technical and organisational capacities to validate simplified proof pursuant to § 4 para 6 last sentence.

#### **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 promulgation of the statutory provisions to be implemented by them; however, they may not enter into force before those statutory provisions.

#### **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 para 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 para 2, the Federal Minister of Digital and Economic Affairs acting with the consent of the Federal Minister of the Interior, the

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. 2 bis 7 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.

Federal Minister of Finance or the Federal Chancellor, depending on whether services relating to the source PIN of natural persons or services relating to the source PIN 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 para 2, the Federal Minister of Digital and Economic Affairs,
4. with respect to § 4a paras 1 to 5, § 4b, § 17 paras 1 and 3 as well as § 18 paras 2 to 7, the Federal Minister of the Interior,
- 4a. with respect to § 4a para 6, § 18 para 3 and § 25 para 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. in all other respects, 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.