The Austrian E-Government Act

Federal Act on Provisions Facilitating Electronic Communications with Public Bodies

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

Art. 1 of the Act published in the Austrian Federal Law Gazette, part I, Nr. 10/2004,
entered into force on 1 March 2004

Table of Contents

Part I
Object and Aims of the Act

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

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

(3) With respect to implementation of the aims of this Federal Act, measures shall be taken to ensure that, by 1 January 2008 at the latest, official Internet sites which provide information or electronic support for procedures are structured in such a way as to comply with international standards for access to the worldwide web, including unhindered access for disabled persons.

Part II
Identification and Authentication in Electronic Communications with Public Bodies
Definitions

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

1. "Identity": designation of a specific person (data subject, No 7) by means of data which are particularly suitable to distinguish persons from each other, such as, in particular, name, date of birth and place of birth but also, for example, company name or (alpha)numerical designations;
2. "Unique identity": designation of a specific person (data subject, No 7) by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects;
3. "Recurring identity": designation of a specific person (data subject, No 7) in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission;
4. "Identification": the process necessary to validate or recognise identity;
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;
6. "Authentication": the process necessary to validate or recognise authenticity;

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 identification number (sourcePIN)”: a number used to identify natural and legal persons and other data subjects which is unmistakably attributable to the data subject to be identified and which, in the case of natural persons, also serves as the basis for generating (private) sector-specific personal identifiers (Paragraphs 9 and 14);
9. “Register of sourcePINs”: a register used for the purpose of uniquely identifying data subjects and comprising the technical components used, where necessary, for the generation of source identification numbers;
10. “Citizen card”: the logical unit, independent of whether implemented on different technical components or not, combining an electronic signature with an identity link (Paragraph 4(2)) and the associated security data and functions plus any existing data on representation.

Identity and Authenticity

3. (1) In the context of electronic communications with controllers in the public sector within the meaning of Paragraph 5(2) of the Datenschutzgesetz 2000 (Data Protection Act 2000), BGBl. I [1] No 165/1999, rights of access to personal data (Paragraph 4 No 1 of the Datenschutzgesetz 2000) in which there is a protected interest in confidentiality within the meaning of Paragraph 1(1) of the Datenschutzgesetz 2000 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. Where only recurring identity can be validated, access may be granted only in respect of those personal data which the person requesting access himself has made available using that same identity.

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

The “Citizen Card” Function

4. (1) The citizen card serves to validate the unique identity of a person making a submission and of the authenticity of a submission made electronically in procedures for which a controller in the public sector has set up a technical environment in which the citizen card can be used.

(2) The unique identification of a natural person who is the lawful holder of a citizen card shall be effected in that person’s citizen card by way of an identity link: the sourcePIN Register Authority (Paragraph 7) shall confirm, by electronic signature, that the natural person identified in the citizen card as the holder has been allocated a particular source identification number (sourcePIN) for the purpose of unique identification. With respect to validation of identity in the event of representation, Paragraph 5 shall apply.

(3) The identity link shall be entered in the citizen card by the sourcePIN Register Authority or, on its behalf, by other authorities or other appropriate bodies to be defined in more detail in the regulation to be adopted pursuant to subparagraph 5. Whether a body is appropriate shall be assessed on the basis of whether it has the requisite technology and the expertise necessary to be able to use it and of whether it can be relied upon to comply with the legal framework conditions.

(4) The authenticity of a submission made using the citizen card shall be validated by the electronic signature contained in the citizen card.

---

[1] “BGBl.” is the abbreviation for Bundesgesetzblatt (Austrian Federal Law Gazette).

(5) Where necessary, detailed rules on subparagraphs 1 to 4 shall be laid down in a regulation of the Federal Chancellor adopted with the consent of any other competent Federal Ministers. The *Länder* (Federal provinces) and the local authorities, the latter represented by the local authorities' association and the municipal authorities' association (*Gemeindebund* and *Städtebund*), shall be consulted prior to adoption of that regulation.

Citizen Card and Representation

5. (1) Where the citizen card is to be used for submissions by a representative, a reference to the permissibility of the representation must be entered in the citizen card of the representative. This occurs where the sourcePIN Register Authority:

1. having been presented with proof of an existing authority to represent or in cases of statutory representation, enters in the citizen card of the representative, upon application by the representative, the sourcePIN of the principal and a reference to the existence of an authority to represent, including any relevant material or temporal limitations; or
2. in cases of professional representation (*berufsmäßige Parteienvertretung*) in which no particular proof of authority to represent is required, enters in the citizen card of the representative, in a form which can be verified electronically, a reference to the fact that he has been authorised to act as professional representative. In those cases, the principal shall be electronically identified pursuant to Paragraph 10(2).

(2) Paragraph 4(3) shall apply *mutatis mutandis* to the entries in the citizen card which are required under subparagraph 1.

(3) Provided that such a service is offered by the local authorities, officials (*Organwalter*) authorised especially for this purpose may, at a person's request, lodge applications for that person with all authorities, irrespective of their material and organisational competence, in procedures in which a citizen card may be used. Applications shall be lodged using the citizen card of the official, the person concerned in the application being electronically identified pursuant to Paragraph 10(2). The general competence of an official to lodge applications for citizens must be apparent from the signature certificate in the official´s citizen card, while the specific instruction issued by the citizen shall be documented by way of certification of the copy of the written application to be kept by the authority in accordance with Paragraph 14 of the Allgemeines Verwaltungsverfahrensgesetz 1991 (General Act on Administrative Procedure 1991).

Source Identification Number

6. (1) The person concerned shall be uniquely identified in the citizen card by his source identification number (sourcePIN).

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

(3) With respect to legal persons and other non-natural persons, the source identification number shall be the number of their entry in the Register of Company Names (Paragraph 3 No 1 of the Firmenbuchgesetz (Register of Company Names Act), BGBl. No 10/1991) or of their entry in the Central Register of Associations (ZVR number) (Paragraph 18(3) of the Vereinsgesetz 2002 (Associations Act 2002), BGBl. No 66/2002) or the registration number allocated in the Supplementary Register (subparagraph 4).

(4) Persons who are not required to be registered in the Central Register of Residents or in the Register of Company Names or in the Register of Associations shall – upon application by them or, in the cases governed by Paragraph 10(2), at the request of the controller of the data file – be registered by the sourcePIN Register Authority (Paragraph No 7) in the Supplementary Register for the purposes of electronic validation of their unique identity. In the case of natural persons, this shall be subject to the condition that proof be provided of the data equivalent to identification data within the meaning of Paragraph 1(5a) of the Meldegesetz 1991 and, in the case of other data subjects, that proof be provided of their legal existence, including their legally valid name. The Supplementary Register shall be divided into sections for natural persons and for other data subjects. The issue of authorities to act on behalf of others may also be entered in the section of the Supplementary Register concerning data subjects who are not natural persons. The domestic or foreign bodies to which proof of the data required for registration in the Supplementary Register may be submitted and the bodies authorised to enter the identity link in the citizen card shall be specified in the regulation of the Federal Chancellor to be adopted pursuant to Paragraph 4(5). Moreover, that regulation shall govern the extent to which the costs caused by contacting the sourcePIN Register Authority and the bodies instructed by it to verify identity in connection with registration in the Supplementary Register and to enter references to representation must be reimbursed; public bodies (*Gebietskörperschaften*) shall in any event be excluded from the duty to reimburse such costs.

(5) For the purpose solely of validating recurring identity, a person may, at his request, be provided with a substitute sourcePIN by the sourcePIN Register Authority, where proof of the data required under subparagraph 3 is not furnished. The substitute sourcePIN shall be generated on the basis of data on the person concerned – for example, name and date of birth and place of birth or serial number of a certificate – which, as a whole, can be expected to distinguish that person sufficiently. It must be possible to recognise the number as a substitute sourcePIN.

(6) The mathematical algorithms applied by the sourcePIN Register Authority in order to generate source identification numbers (using strong cryptography in the case of natural persons) and substitute source identification numbers (hash value of the data and additional strong cryptography in the case of natural persons) shall be determined by the sourcePIN Register Authority and – with the exception of the cryptographic key used – published on the Internet.

sourcePIN Register Authority

7. (1) The sourcePIN Register Authority is the Data Protection Commission, which shall perform that function by way of the Register for Data Files**.**

(2) In maintaining the Supplementary Register, generating source identification numbers and conducting the procedures governed by Paragraphs 4, 9 and 10, the sourcePIN Register Authortiy shall have recourse to the services of the Federal Ministry of the Interior, insofar as natural persons are concerned, and of the Federal Ministry of Finance, insofar as all other data subjects are concerned. The detailed provisions governing the distribution of functions between the Data Protection Commission in its capacity as sourcePIN Register Authority and the Federal Ministry of the Interior or the Federal Ministry of Finance as service providers shall be laid down in a regulation of the Federal Chancellor after consultation of the Data Protection Commission and with the consent of, as appropriate, the Federal Minister of the Interior or the Federal Minister for Finance.

Unique Identification in Data Files

8. In data files of controllers in the public sector, the identification of natural persons within the framework of the citizen card scheme may be represented only in the form of a sector-specific personal identifier (Paragraph 9). With respect to persons who are not natural

persons, the source identification number may be stored for the purpose of unique identification.

Sector-Specific Personal Identifiers

9. (1) The sector-specific personal identifier is derived from the source identification number of the natural person concerned. The use of that derived identifier for identification purposes shall be limited to that sector of State activity which is served by the data file in which the personal identifier is to be used (sector-specific personal identifier, ssPIN). The specific sector of State activity to which a data file is to be allocated shall – to the extent that it is not governed by Paragraph 17(2) Nos 1 to 3 or (3) – be made apparent in its registration in the Register of Data Files resp. in the Standard- und Muster-Verordnung (Regulation on Standard and Model Data Processing) provided for in Paragraph 17(2) No 6 of the Datenschutzgesetz 2000.

(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 uses of data (Paragraph 6(1) No 2 of the Datenschutzgesetz 2000) within the same area. The description and delimitation of those areas shall be determined in a regulation of the Federal Chancellor. The *Länder* and the local authorities, the latter represented by the local authorities' association and the municipal authorities' association, shall be consulted prior to adoption of that regulation.

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

Generation of Sector-Specific Personal Identifiers

10. (1) A person's ssPIN shall be generated by the use of the citizen card in electronic procedures for which a controller in the public sector has created an environment in which the citizen card may be used.

(2) Sector-specific personal identifiers may be generated without the use of a citizen card only by the sourcePIN Register Authority and this is permissible only where unique identification on the basis of the ssPIN in data files of controllers in the public sector is necessary because personal data are to be processed or transmitted in conformity with the Datenschutzgesetz 2000. Such cases include, in particular, administrative cooperation, data acquisition at the request of the data subject or a submission to an authority by a professional representative. In the event of a request of ssPINs for a sector in which the body making the request is not authorised to act as authority (external ssPINs) or in the case of a request for an ssPIN made by a professional representative, only ssPINs which have been encrypted in accordance with Paragraph 13(2) may be made available.

(3) The reimbursement of the costs of the supply of sector-specific personal identifiers in connection with professional representation pursuant to subparagraph 2 shall also be governed by the regulation to be adopted pursuant to Paragraph 4(5).

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 Identification Number of Natural Persons

12. (1) Insofar as source identification numbers do not contain public data, such as the number of an entry in the Register of Company Names or the ZVR number, their confidentiality shall be subject to special protection by way of the following measures of the citizen card scheme:

1. The number derived from the CRR number and used as the source identification number of natural persons may be permanently stored only in the citizen card and only in connection with the identity link or in order to indicate an instance of authority to represent.
2. Source identification numbers of natural persons shall be generated in the sourcePIN Register whenever they are required. They shall not, however, be subject to storage exceeding the time necessary for generation and immediate transaction.
3. The use of the source identification number of natural persons in order to generate the ssPIN may not give rise to any storage of the source identification number outside of the generation process.
4. The generation of an pssPIN (Paragraph 14) on the basis of the source identification number may not be carried out by a controller in the private sector.

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

1. with the cooperation of the data subject by use of his citizen card; in each case, the data subject must be informed accordingly of the electronic activation of the citizen card functions, or,
2. without the cooperation of the data subject, by the sourcePIN Register Authority in accordance with the detailed provisions of Paragraphs 10 and 13(2).

Further Guarantees for the Protection of Personal Identifiers

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

(2) Where it is permissible under Paragraph 10(2) to request from the sourcePIN Register Authority a sector-specific personal identifier for the purpose of the unique identification of a data subject, the sourcePIN Register Authority may, insofar as an external ssPIN is concerned - this is an ssPIN for a sector in which the requesting party has no competence to act as authority - make the ssPIN available only in encrypted form. The form of that encryption must be such as to ensure that:

1. only the controller in whose data file it is permissible to use the ssPIN in decrypted form is able to decrypt it (subparagraph 3); and
2. as a result of the inclusion in the basis for encryption of additional variable data of which the requesting party has no knowledge, the ssPIN cannot, even in encrypted form, supply any information on the data subject.

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

Part III

Use of the Citizen Card Functions in the Private Sector

Private Sector-Specific Personal Identifiers

14. (1) In order to identify natural persons in electronic communications with a controller in the private sector (Paragraph 5(3) of the Datenschutzgesetz 2000), a specific number may be derived, using the citizen card, from the hash value generated from the source identification number of the data subject and the source identification number of the controller as sector code (private sector-specific personal identifier, pssPIN). This shall be subject to the condition that the controller in the private sector has set up a technical environment in which

the citizen card can be used and in which the controller´s source identification number is made available as the sector code for generation of the pssPIN.

(2) Controllers in the private sector may store and use only such private sector-specific personal identifiers as have been generated using their own source identification number as sector code.

Guarantees for the Protection of Source Identification Numbers and Personal Identifiers

15. (1) A private sector-specific personal identifier may be generated only with the cooperation of the data subject on the basis of the citizen card; in each case, the data subject must be informed accordingly of the electronic activation of those functions.

(2) The source identification number of the data subject may not be made available to a controller in the private sector by way of the citizen card functions at any time during the generation of the pssPIN. Electronic verification of the accuracy of the identity link used by the data subject is however possible by submitting a request for access to the Central Residents Registry under Paragraph 16(1) of the Meldegesetz 1991.

Part IV

Electronic Validation of Data

Information on Economic Activity 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 Registry under Paragraph 114(2) of the Bundesabgabenordnung (Federal Fiscal Code).

(2) Where validation of the data referred to in subparagraph 1 is required in procedures involving a controller in the public sector, the data subject may himself supply it by submitting a copy signed electronically by the Documentation Registry 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.

Data concerning Personal Status and Nationality

17. (1) Where the accuracy of the 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 Residents Registry 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) Where other authorities must determine, as a preliminary question in a procedure, the accuracy of data relating to personal status or nationality which are also registration data, they may, provided that the person concerned has consented to acquisition of the data or that such acquisition through official channels is authorised by statute, submit an electronic request to the Central Residents Registry in that regard, which is to be treated in accordance with Paragraph 16a(4) of the Meldegesetz 1991.

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

1. consenting to the acquisition of the data required from the Central Residents Registry in procedures in which it is necessary to submit standard documents within the meaning of subparagraph 1; or

2. requesting from the Central Residents Registry a confirmation of registration which has been signed electronically with an official signature (Paragraph 19) and which states that the accuracy of the individual registration data has been verified.

Other Data

18. Authorities or persons on whom public powers have been conferred shall make public on the Internet the extent to which they are prepared to issue electronic validation of the data stored by them within their area of competence or operations. Validation which refers to personal data may be issued only to the person concerned himself, or to third parties with the consent of the data subject only, unless acquisition of the data through official channels is authorised by statute.

Part V

Peculiarities of Keeping Electronic Records

Official Signature

19. (1) An official signature, being the electronic signature of a public authority, is an electronic signature within the meaning of the Signaturgesetz (Signature Act), the peculiarity of which is indicated by an appropriate attribute in the signature certificate.

(2) Official signatures serve to facilitate recognition of the fact that a document originates from an authority. Such signatures may therefore be used only by authorities, in accordance with the detailed conditions laid down in subparagraph 3, when signing electronically or drawing up the documents issued by them.

(3) The official signature shall be represented in the electronic version of the document by an image which the authority has published on the Internet in secure form as its own. In addition to the image, the electronic version must also show at least the serial number and the name and country of origin of the certification service provider as well as the actual value of the signature. It must be possible to verify the signature by converting the representation of the entire document into a form which enables the signature to be verified. The additional information required in order to retrieve the electronic document from the representation must likewise be published on the Internet in secure form by the issuer of the document.

Probative Value of Printouts

20. There shall be a presumption that electronic documents of authorities printed on paper are genuine if the document is signed with an official signature and it is possible to verify the signature even in printed form by reconstructing the electronic version of the document. For that purpose, the document must state that it may be reconstructed and contain a reference to the source on the Internet where the procedure for reconverting the printout into electronic form and the applicable verification mechanisms are explained.

Submission of Electronic Records

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

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

(3) Where the authority to which the electronic record is to be submitted has authorised an electronic delivery service to receive correspondence addressed to it, the record may also be submitted to that agent, in particular, where proof of submission is required. In such cases, the provisions in Part III of the Zustellgesetz (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 VI

Penal Provisions

Prohibited Use of Source Identification Numbers, Sector-Specific Personal Identifiers or Official Signatures

22. (1) Insofar as an act does not constitute a criminal offence which falls within the jurisdiction of the courts or 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 and III, obtains the source identification number or sector-specific personal identifier of a natural person with a view to using them in order to acquire unlawfully personal data of the data subject; or
2. stores or uses a private sector-specific personal identifier of another controller in the private sector without authorisation; or
3. makes available to other controllers in the private sector a private sector-specific personal identifier derived from his own source identification number in a manner prohibited under Paragraph 8 of the Datenschutzgesetz 2000; or
4. uses a private sector-specific personal identifier in order to supply third parties with data concerning a registered domicile of the data subject; or
5. uses or purports to use an official signature contrary to Paragraph 19(2).

(2) The penalty of forfeit of objects (Paragraphs 10, 17 und 18 of the Verwaltungsstrafgesetz 1991 (Administrative Offences Act)) which have been acquired in connection with an administrative offence within the meaning of subparagraph 1 may be imposed.

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

Part VII

Transitional and Final Provisions

Linguistic Equal Treatment

23. Insofar as the terms in this Article referring to natural persons are worded only in the masculine form, they shall apply to men and women equally.

Entry into Force

24. 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.

Transitional Provisions

25. (1) Until 31 December 2007, administrative signatures may also be used in connection with citizen card functions and shall be treated in the same way as secure signatures. Administrative signatures are signatures which, within the limits of the scope of their permissible use, provide sufficient security even if they do not necessarily satisfy all the conditions for the generation and storage of data used to create secure signatures and are not necessarily based on a qualified certificate. The security and organisational conditions which must be fulfilled by an administrative signature for the purposes of this Federal Act shall be laid down in a regulation of the Federal Chancellor.

(2) In cases in which laws beneath the constitutional level expressly require the use of a secure electronic signature in communications with public bodies exercising official authority (*Hoheitsverwaltung)*, that condition shall be regarded as fulfilled even where an administrative signature is used, until expiry of the transitional period referred to in subparagraph 1.

Adoption and Entry into Force of Regulations

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

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 organs shall be competent to implement this Federal Act:

1. with respect to Paragraph 4(5), the Federal Chancellor acting with the consent of any other competent Federal Ministers,
2. with respect to Paragraph 7(2), the Federal Chancellor acting with the consent of the Federal Minister of the Interior or the Federal Minister of Finance, depending on whether services relating to the source identification numbers of natural persons or services relating to the source identification numbers of non-natural persons are concerned,
3. with respect to Paragraph 9(2), the Federal Chancellor,
4. with respect to the final sentence of Paragraph 15(2) and Paragraph 17, the Federal Minister if the Interior,
5. with respect to Paragraph 16, the Federal Minister of Finance,
6. as regards the remainder, any Federal Minister within his area of competence and to the extent that implementation is not a matter for the Federal Government or the Governments of the *Länder*.