Übersetzung durch den Sprachendienst des Bundesministeriums des Innern.
Translation provided by the Language Service of the Federal Ministry of the Interior.
Stand: Die Übersetzung berücksichtigt die Änderung(en) des Gesetzes durch Artikel 4 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2959)
Version information: The translation includes the amendment(s) to the Act by Article 4 of the Act of 22 December 2011 (Federal Law Gazette I p. 2959)

Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG)

Act on Identity Cards of 18 June 2009 (Federal Law Gazette I, p. 1346), amended by Article 4 of the Act of 22 December 2011 (Federal Law Gazette I, p. 2959)

Part 1
General provisions

Section 1
Identification requirement; law on identification documents

(1) Germans as defined in Article 116 (1) of the Basic Law shall be required to possess an identity card once they have reached the age of 16 and are subject to the general registration requirement, or if not subject to this requirement, then if they mainly reside in Germany. They must present their identity card at the request of an authority entitled to check identification. Identity card holders may not be required to deposit their identity card or otherwise surrender possession. This shall not apply to authorities entitled to check identification nor in case of withdrawal or confiscation.
(2) The identification requirement shall also apply to persons subject to a special registration requirement under state laws on registration as masters of inland vessels or as seamen. It shall not apply to persons serving a custodial sentence. Persons with a valid passport as defined in Section 1 (2) of the Passport Act may satisfy the identification requirement under subsection 1 first and second sentence also by possessing and presenting their passport.
(3) The responsible identity card authority under Section 7 (1) and (2) may waive the identification requirement for certain persons

1. for whom a guardian has been appointed not only by provisional order, or who are incapable of acting or giving consent and are represented by an authorized representative having a notarially certified power of attorney,

2. who are permanent residents of a hospital, nursing home or similar facility, or

3. who are unable to travel without assistance due to a permanent disability.

(4) Upon application, an identity card shall be issued for

1. persons under age 16, and

2. Germans as defined in Article 116 (1) of the Basic Law who are not subject to the general registration requirement because they have no residence in Germany.

Section 2
Definitions

(1) Identity cards as defined in this Act shall be the national identity card and the temporary national identity card.
(2) As defined in this Act, authorities entitled to check identification shall be public bodies authorized to determine the identity of persons as a official measure to fulfil their legally assigned duties.
(3) Service providers shall be natural and legal persons who, to carry out tasks of the public administration or for own business purposes, require proof of identity or individual identifying features of the identity card holder and who have their place of residence, business or office within the geographical area covered by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data or in other countries having a comparable standard of data protection.
(4) An authorization certificate shall be an electronic certificate which enables a service provider

1. to verify its identity vis-à-vis the identity card holder and

2. to request the transmission of personal and identity-card-related data from the identity card.

Authorized service providers shall be issued authorization certificates. Authorities entitled to check identification shall be issued official authorization certificates to be used only for the official task of checking identification.
(5) A service- and card-specific identifier shall be a series of characters generated in the storage and processing medium of the identity card. It shall allow the service provider to electronically identify the identity card for which it was generated without having to transmit additional personal data.
(6) The blocking code shall be a series of characters used only to block lost or stolen identity cards whose electronic identification function has been activated.
(7) Blocking attributes of an identity card shall be service- and card-specific series of characters which the service provider for whom they were generated use only to identify lost or stolen identity cards.
(8) Each identity card shall be issued a new serial number. The serial number of an identity card shall consist of a four-digit authority ID number and a five-digit, randomly assigned number, and may include both numerals and letters. The serial number of a temporary identity card shall consist of one letter and seven numerals.
(9) The check digits shall be generated from the data of the machine-readable area and shall serve as an indication of its integrity.
(10) The PIN code shall be a six-digit number used to approve the transmission of data from the identity card for the purpose of electronic identification.
(11) The access code shall be a randomly generated six-digit number printed on the card to protect against unauthorized interception of communications between the identity card and card readers.
(12) The PUK code shall be a randomly generated number to unblock the identity card after the incorrect PIN code has been entered three times in succession.

Section 3
Temporary identity cards

(1) A temporary identity card shall be issued to any applicant who provides a credible reason for immediately requiring an identity card.
(2) Only the authorities specified in Section 7 (1) shall be responsible for issuing temporary identity cards.

Section 4
Ownership; card manufacturer; authority responsible for issuing authorization certificates

(1) No one may have more than one valid identity card issued by the Federal Republic of Germany.
(2) Identity cards shall be the property of the Federal Republic of Germany.
(3) The Federal Ministry of the Interior shall determine the card manufacturer, the authority responsible for issuing authorization certificates and the administrator of revocation lists and shall publicize their names in the Federal Gazette.

Section 5
Models; stored data

(1) Identity cards shall be issued in accordance with uniform models.
(2) In addition to the issuing authority, date of issue, date of expiry, access number and the data listed in subsection 4 second sentence, identity cards shall clearly indicate only the following information about the card holder:

1. family name and name before marriage,
2. given names,
3. doctoral degree
4. date and place of birth,
5. photograph,
6. signature,
7. height,
8. eye colour,
9. address; in case of an address outside Germany, then the statement "no main residence in Germany",
10. nationality,
11. serial number, and
12. religious name / stage or pen name.

(3) Temporary identity cards shall include the information in subsection 2 nos. 1 through 12 as well as the issuing authority, date of issue and date of expiry.
(4) Identity cards shall have a machine-readable area. This area shall contain only the following clearly printed information:

1. Abbreviations
   a) "IDD" for identity card of the Federal Republic of Germany or
   b) "ITD" for temporary identity card of the Federal Republic of Germany,
2. family name,
3. given names,
4. serial number,
5. "D" for German nationality,
6. date of birth,
7. date of expiry,
8. check digits, and

9. empty spaces.

When verifying identity pursuant to Section 17, the printed access code may be machine-read as well.

(5) Identity cards shall contain an electronic storage and processing medium on which the following data shall be stored:

1. the data listed in subsection 2 nos. 1 through 5, 9 and 12.

2. the data of the machine-readable area according to subsection 4 second sentence, and

3. fingerprints pursuant to subsection 9 and information on which fingers were used for fingerprinting and on the quality of the prints.

(6) The stored data shall be secured against unauthorized alteration, deletion and retrieval.

(7) In derogation from subsection 5, children under age 6 shall be issued identity cards with an electronic storage and processing medium on which only a photograph and the data of the machine-readable area according to subsection 4 second sentence are stored.

(8) The serial number, check digits, blocking code and blocking attributes may not contain any of the identity card holder's personal data or reference to such data.

(9) Fingerprints shall be stored only at the request of the card applicant. The applicant's fingerprints shall be stored on the identity card's electronic storage and processing medium as flat prints of the left and right index fingers. In case of a missing index finger, injured fingertip or poor-quality print, a flat print of the thumb, middle or ring finger shall be stored instead. Fingerprints shall not be stored if it is not possible to take prints for medical reasons of a more than temporary nature.

(10) The data stored on the electronic storage and processing medium shall also enable the electronic identification function pursuant to Section 18.

Section 6
Length of validity; early application; geographical restrictions

(1) Identity cards shall be valid for a period of ten years.

(2) Before an identity card expires, the card holder may apply for a new one if he or she demonstrates a legitimate interest in having a new one issued.

(3) For persons under age 24, identity cards shall be valid for a period of six years.

(4) The length of validity for temporary identity cards shall be based on the purpose of use; it may not exceed three months.

(5) The length of validity shall not be extended.

(6) In the cases referred to in Section 29 of the Nationality Act, an identity card shall not be valid past the holder's 23rd birthday until the responsible authority has determined whether the holder may retain his/her German citizenship.

(7) In accordance with the requirements of Section 7 (1) of the Passport Act, the responsible authority may order in individual cases that the identity card does not entitle the holder to leave Germany.

(8) Orders pursuant to subsection 7 may be recorded in the border police database.

Section 7
Administrative responsibility

(1) The identity card authorities designated by the Länder shall be responsible for matters related to identity cards in Germany.

(2) The Federal Foreign Office and its designated diplomatic missions abroad shall be responsible for matters related to identity cards outside Germany.

(3) The identity card authorities, diplomatic missions abroad and authorities entitled to make official checks of identification shall be responsible for withdrawal pursuant to Section 29 (1) and for confiscation pursuant to Section 29 (2).

(4) The authority responsible for issuing authorization certificates pursuant to Section 4 (3) shall be responsible for issuing and suspending certificates pursuant to Section 21. The administrator of revocation lists pursuant to Section 4 (3) shall be responsible for keeping a revocation list pursuant to Section 10 (4) first sentence.
(5) The bodies responsible for compliance with data protection regulations shall be responsible for service providers in Germany. If service providers have their place of residence, business or office outside Germany, the Federal Commissioner for Data Protection and Freedom of Information shall be the responsible data protection supervisory authority as referred to in Section 21 (5) third sentence.

Section 8
Local responsibility; lack of local responsibility

(1) In Germany, the identity card authority in the district in which the identity card applicant or holder is required to register his/her residence or main residence shall have local responsibility. If the applicant does not have a place of residence, then the identity card authority in the district where the applicant is temporarily staying shall have local responsibility.
(2) Outside Germany, the diplomatic missions abroad designated by the Federal Foreign Office in the district in which the identity card applicant or holder is usually resident shall have local responsibility. Identity card holders shall provide proof of their usual place of residence.
(3) For masters of inland vessels who have no residence in Germany, the identity card authority of the place where the vessel is registered shall have local responsibility; for seamen who have no residence in Germany, the identity card authority of the place where the vessel's owner has its headquarters shall have local responsibility.
(4) An identity card application must also be processed by an identity card authority which does not have local responsibility if there is a compelling reason to do so. Identity cards may be issued only with the permission of the locally responsible identity card authority.

Part 2
Issuing and blocking the identity card

Section 9
Issuing the identity card

(1) Identity cards shall be issued upon application to Germans within the meaning of Article 116 (1) of the Basic Law. Section 3a (1) of the Administrative Procedure Act shall not apply. During the application process, information to be provided following the initial application may be submitted electronically. An authorized representative may not file an identity card application on behalf of the passport applicant or his/her legal representative. This shall not apply to an applicant who is unable to act or provide consent, upon presentation of a power of attorney which has been publicly certified or notarized for this purpose. The applicant and his legal or authorized representative are to appear in person.
(2) For minors under age 16 and for persons who are legally incapable and who do not have an authorized representative in accordance with subsection 1 fifth sentence, the only person who may file an application on their behalf is the custodial adult responsible for supervising their residency. After the minor's 16th birthday and before his or her 18th birthday, the custodial adult shall be required to submit an application for an identity card if the minor fails to do so. Minors 16 years old or older may undertake proceedings pursuant to this Act.
(3) This application shall include all information needed to confirm the applicant’s identity and status as a German citizen. Information about doctoral degrees attained and any religious, stage or pen names shall be voluntary. The applicant shall supply the necessary supporting documents. When submitting an application, applicants shall indicate in writing whether their fingerprints are to be stored on the storage and processing medium of the identity card. If the applicant decides against storing his/her fingerprints, this shall result in no legal or factual disadvantages other than that procedures for verifying identity by checking fingerprints

cannot be used. Applicants shall be informed in writing of this and of the fact that storing fingerprints is voluntary. If fingerprints are to be stored on the identity card, they are to be taken from the applicant and captured electronically in accordance with Section 5 (9). No fingerprints of children under age 6 shall be taken.
(4) In case of doubt regarding the applicant's identity, the necessary measures to establish his/her identity shall be taken The identity card authority may arrange to have applicants photographed and fingerprinted by the police if it would otherwise be impossible or extremely difficult to determine the applicant's identity. Once the applicant's identity has been established, any documents collected for the purpose of establishing such identity shall be destroyed. The fact that these documents have been destroyed shall be recorded.
(5) A child aged 10 or over at the time the application is made shall sign his/her own identity card.

Section 10
Deactivating; activating; blocking and unblocking the electronic identification function

(1) When applicants pick up their identity cards, they shall state in writing to the identity card authority whether they intend to use the electronic identification function. Card holders may change this statement at any time during the card's period of validity by writing to the identity card authority. If applicants do not wish to use the electronic identification function, the identity card authority shall deactivate this function. If the application is submitted at a diplomatic mission abroad, the applicant shall submit his/her statement with the application for an identity card.
(2) The card manufacturer shall deactivate the electronic identification function before the identity card is handed over if applicants have not yet turned 16 at the time of application. The same shall apply when the statement pursuant to subsection 1 fourth sentence is submitted at a diplomatic mission abroad and the applicant has declared that he/she does not wish to use the electronic identification function.
(3) During the card's period of validity, card holders aged 16 and over may request to have a deactivated electronic identification function activated. They may also request to have an activated electronic identification function deactivated.
(4) The administrator of revocation lists pursuant to Section 7 (4) second sentence shall provide, via public communication channels available at all times, every service provider with a current list (revocation list), drawn up specifically for that service provider, of lost or stolen identity cards having an activated electronic identification function. Service providers shall regularly consult their revocation lists and check them locally with regard to the electronic identification function against identity cards to be accepted.
(5) If the issuing identity card authority becomes aware that

1. an identity card with an activated electronic identification function has been lost or stolen, or

2. a card holder has passed away,

it shall immediately inform the administrator of revocation lists pursuant to Section 7 (4) second sentence of the blocking code for the identity card in question, for the purpose of updating the revocation list.
(6) A card holder whose identity card having an activated electronic identification function has been lost or stolen may also report the blocking code to the administrator of revocation lists pursuant to Section 7 (4) second sentence in order to immediately block the electronic identification function. The requirement to report the loss or theft of the identity card to the identity card authority in accordance with Section 27 (1) no. 3 shall remain unaffected.
(7) The administrator of revocation lists pursuant to Section 7 (4) second sentence shall provide a blocking service, via public communication channels available at all times, to the identity card authorities for the cases pursuant to subsection 5 and to card holders for the cases pursuant to subsection 6.

(8) If, after blocking has been carried out in accordance with subsection 5 or 6, the card holder reports in accordance with the conditions of Section 9 (1) sixth sentence that the identity card has been located and presents the card, the identity card authority shall request the administrator of revocation lists pursuant to Section 7 (4) second sentence to unblock this identity card. The requirement of the card holder to present the identity card after locating it in accordance with Section 27 (1) no. 3 shall remain unaffected.
(9) The identity card authority or the police shall record the time the loss or theft of the identity card was reported and shall inform the issuing identity card authority.

Section 11
Information obligations

(1) At the card holder's request, the identity card authority shall allow the card holder to inspect the retrievable data stored on the electronic storage and processing medium.
(2) At the time of application, the identity card authority shall provide card applicants with information on the electronic identification function, so that they are prepared to make the statement referred to in Section 10 (1).
(3) The identity card authority shall inform card applicants in writing of the measures necessary to ensure the secure use of the electronic identification function.
(4) Card applicants shall confirm in writing that they have read and understood the information referred to in subsections 2 and 3.
(5) Identity card authorities that become aware of the loss or theft of an identity card shall immediately inform the responsible identity card authority, the issuing identity card authority and the police; if the police otherwise become aware of the loss or theft of an identity card, they shall immediately inform the responsible and the issuing identity card authorities. In doing so, they shall provide the family name, given names, serial number, issuing identity card authority, date of issue and date of expiry of the identity card. The police shall enter the identity card in their register of missing and stolen property.
(6) If an identity card authority that is not responsible pursuant to Section 8 (4) issues an identity card, it shall provide the responsible identity card authority with the family name, given names, date and place of birth, issuing identity card authority, date of issue, date of expiry and serial number of the card.
(7) An identity card authority shall inform the issuing identity card authority immediately whenever it activates or deactivates the electronic identification function.

Section 12
Forms and procedures for collecting, checking and transmitting data

(1) Data needed for the production of identity cards, in particular all data from identity card applications, shall be sent from the identity card authorities to the card manufacturer via electronic data transmission. The data may also be transmitted via intermediary agencies. The bodies concerned shall take state-of-the-art measures to ensure data protection and data security, in particular to guarantee the confidentiality and integrity of the data and the identification of the transmitting body; when publicly accessible networks are used, state-of-the-art encryption methods shall be applied.
(2) For the electronic capture and quality assurance of the photograph and fingerprints, and for transmission of identity card application data from the identity card authority to the card manufacturer, only those technical systems and components may be used which meet the requirements of Section 34 no. 3 of the statutory instrument. The Federal Office for Information Security shall ensure compliance with the requirements in accordance with Section 34 no. 4 of the statutory instrument.

Section 13
Transmitting PIN codes, PUK codes and blocking codes

The card manufacturer shall send card applicants the PIN code, PUK code and blocking code for the identity card in order to use, block and unblock the electronic identification function. The PIN code shall be sent separately from the other documents. If the card

applicant presents legitimate grounds for doing so, the documents referred to in the first sentence shall be sent to the identity card authority which hands out the identity card. This authority shall provide the card holder with the documents. The identity card authority shall inform the card holder of the risks of this process at the time of application.

Part 3
Personal data

Section 14
Collecting and using personal data

Personal data may be collected and used from or with the help of the identity card only by

1. authorities entitled to check identification in accordance with Sections 15 through 17,

2. public- and private-sector bodies in accordance with Sections 18 through 20.

Section 15
Automated retrieval and storage by authorities entitled to check identification

(1) Authorities entitled to check identification may not use identity cards for the automated retrieval of personal data. In derogation from the first sentence, federal and state police authorities and offices, customs administration authorities and state tax investigation units may, within the framework of their duties and powers, use identity cards for the automated retrieval of personal data stored in police databases for the following purposes:

1. border control,

2. alerts or to establish a person's whereabouts for the purpose of criminal prosecution, enforcement of a criminal sentence or to prevent threats to public security, and

3. customs control as part of police surveillance.

No subject-related record of database searches that have not yielded any results may be kept, except as provided in legal provisions enacted in accordance with subsection 2.
(2) In the cases referred to in subsection 1, unless the law provides otherwise, personal data may not be stored in databases when the identity card is read automatically; this shall also apply to searches of police databases that have yielded results.

Section 16
Use of serial numbers, blocking codes and blocking attributes by authorities entitled to check identification

Authorities entitled to check identification may not use serial numbers, blocking codes or blocking attributes in such a way that they can be used to enable the automated retrieval of personal data or to establish connections between data files. In derogation from the first sentence, the following may use serial numbers for the following purposes:

1. identity card authorities in order to retrieve personal data from their databases, and

2. federal and state police authorities and offices, state tax investigation units and the agencies of the customs investigation service in order to retrieve the serial numbers of identity cards which have been lost or declared invalid or which are suspected of being used by unauthorized persons.

Section 17
Checking identity using data stored on the electronic storage and processing medium

Authorities entitled to check identification may retrieve and use data stored on the electronic storage and processing medium of the identity card only for the purpose of checking the

authenticity of the document or the identity of the card holder and only in accordance with the third and fourth sentences. Checks of authenticity or identity via public communication channels shall not be permitted. If the law enforcement or customs authorities, state tax investigation units, identity card, passport or registration authorities may check the authenticity of the identity card or the identity of the card holder, they shall be authorized to retrieve biometric and other data stored on the electronic storage and processing medium of the identity card, to collect the necessary biometric data from the identity card holder and to compare these biometric data. The data collected in accordance with the third sentence shall be erased immediately after the authenticity of the identity card or the identity of its holder has been checked.

Section 18
Electronic identification

(1) Identity card holders aged 16 or over may use their identity cards to verify their identity vis-à-vis public and private-sector bodies electronically. In derogation from the first sentence, electronic identification shall not be permitted if the conditions of Section 3a (1) of the Administrative Procedure Act, of Section 87a (1) first sentence of the German Fiscal Code or Section 36a (1) of the Social Code, First Book are not met.
(2) Electronic identification shall take place via transmission of data from the electronic storage and processing medium of the identity card. State-of-the-art technical measures shall be taken to ensure data protection and data security, in particular ensuring data confidentiality and integrity. If generally accessible networks are used, encryption shall be applied. Persons other than the identity card holder shall not be permitted to use the electronic identification function.
(3) The blocking attribute and the indication as to whether the identity card is valid shall always be transmitted for checking whether the identity card has expired or been blocked. The following additional data may be transmitted:

1. family name,
2. given names,
3. doctoral degree
4. date of birth,
5. place of birth,
6. address,
7. type of document,
8. service- and card-specific identifier,
9. the abbreviation “D” for the Federal Republic of Germany,
10. indication whether the card holder is older or younger than a particular age,
11. indication whether a place of residence matches the requested place of residence, and
12. religious name / stage or pen name.

(4) Data shall be transmitted only if the service provider transmits a valid authorization certificate to the identity card holder, who then enters his/her PIN code. Before the card holder enters the PIN code, the following information from the authorization certificate must be transmitted for display:

1. name, address and e-mail address of the service provider,

2. categories of data to be transmitted pursuant to subsection 3 second sentence,

3. purpose of the transmission,

4. indication of the bodies responsible for the service provider checking compliance with data protection regulations,

5. the authorization certificate's date of expiry.

(5) Transmission shall be limited to the data categories listed on the authorization certificate. In individual cases, the identity card holder may refuse the transmission of data also in these categories.

Section 19
Storage using electronic identification

(1) It shall be permitted to save a blocking attribute only

1. for lost or stolen identity cards on the revocation list pursuant to Section 10 (4) first sentence, or

2. temporarily with the service provider to check whether the identity card is listed on the revocation lists pursuant to Section 10 (4) first sentence; the data shall be erased immediately after checking. To enable repeated checks as to whether the identity card is listed on the revocation lists pursuant to Section 10 (4) first sentence, in derogation from this provision a service provider verifying identity in accordance with the Money Laundering Act, the Electronic Signature Act or the Telecommunications Act shall not erase a saved blocking attribute until one week after it was first saved.

(2) It shall be permitted to save a blocking code only in the identity card register pursuant to Section 23 (3) no. 12.
(3) It shall not be permitted to save all blocking codes or all blocking attributes centrally.
(4) Data transmitted to service providers for technical reasons or for comparison with the revocation list while checking identity electronically may be saved only for the length of transmission. Processing of data pursuant to Section 18 (3) second sentence shall remain unaffected.

Section 20
Use by public- and private-sector bodies

(1) The card holder may use the identity card as proof of identity and authorization document vis-à-vis public- and private-sector bodies.
(2) Public- and private-sector bodies may use the identity card only to verify identity electronically and not for the automated retrieval or storage of personal data.
(3) Serial numbers, blocking codes and blocking attributes may not be used to enable the automated retrieval of personal data or to link data files. This shall not apply to service providers checking blocking attributes for the purpose of checking whether an identity card's electronic identification function has been blocked.

Part 4
Authorizations; electronic signature

Section 21
Issuing and suspending authorizations of service providers

(1) Under the conditions of subsection 2, upon written application service providers shall be authorized to request the data necessary to perform their tasks or business via electronic identification of the identity card holder using an authorization certificate. The responsible body pursuant to Section 7 (4) first sentence shall issue the authorizations to service providers in accordance with the following provisions, and shall issue service providers with the necessary authorization certificates via public communication channels available at all

times. The application shall contain the data pursuant to Section 18 (4) second sentence nos. 1 through 4.
(2) Authorization pursuant to subsection 1 shall be issued if

1. the purpose given is not unlawful;

2. the purpose does not consist of commercial transmission of the data, and no indications of commercial or unauthorized transmission of the data exist;

3. the service provider submitting the application has demonstrated the need for the data to be transmitted for the purpose described;

4. the requirements, in particular of data protection and data security, in accordance with Section 34 no. 7 of the statutory instrument, are met; and

5. there are no indications that the authorization will be misused.

The service provider shall voluntarily agree to confirm the requirements pursuant to no. 4 in writing and to demonstrate compliance upon request.
(3) The authorization shall be valid for a limited period. The length of validity may not exceed three years. The authorization may be used only by the service provider specified in the authorization certificate and only for the purpose specified therein. The authorization may be made subject to additional conditions and renewed upon application.
(4) Changes to the data and information pursuant to subsection 1 third sentence shall be reported immediately to the responsible body pursuant to Section 7 (4) first sentence.
(5) The authorization shall be withdrawn if it was issued on the basis of false or incomplete information given by the service provider. It shall be revoked if it should not have been issued at all or not with the same extent. The authorization should be withdrawn or revoked if the data protection supervisory authority responsible for the service provider so requests because there is reason to believe that the service provider has unlawfully processed or used personal data received on the basis of the authorization certificate.
(6) After notification that the authorization has been withdrawn or revoked, the service provider may no longer use any authorization certificates in its possession. This shall not apply as long and to the extent that immediate enforcement (Section 30) has been suspended.

Section 22
Electronic signature

Identity cards shall be designed as secure signature creation devices as referred to in Section 2 no. 10 of the Electronic Signature Act. The provisions of the Electronic Signature Act shall remain unaffected.

Part 5
Identity card register; storage provisions

Section 23
Identity card register

(1) The identity card authorities shall keep a register of identity cards.
(2) The identity card register shall serve the implementation of this Act, in particular

1. issuing identity cards and verifying their authenticity,

2. verifying the identity of the card holder or the person to whom the card was issued,

(3) In addition to the photograph and signature of the card holder and the necessary processing notes, the identity card register shall contain only the following data:

1. family name and name before marriage,

2. given names,

3. doctoral degree

4. date of birth,

5. place of birth,

6. height,

7. eye colour,

8. address,

9. nationality,

10. family name, given name(s), date of birth and signature of legal representatives,

11. serial number,

12. blocking code,

13. date of expiry,

14. issuing authority,

15. notes on instructions pursuant to Section 6 (7),

16. information concerning the card holder's obligation to furnish a declaration pursuant to Section 29 of the Nationality Act,

17. whether the identity card's electronic identification function has been deactivated and whether the identity card is on the revocation list,

18. religious name, stage or pen name and

19. statement of authorization issued pursuant to Section 8 (4) second sentence.

(4) Personal data in the identity card register shall be kept at least until a new identity card is issued but no longer than five years after the identity card in question has expired, when they shall be deleted. Identity card authorities pursuant to Section 7 (2) with consular responsibilities shall retain such data for 30 years.
(5) The responsible identity card authority shall provide proof of identity cards for which it issued authorization pursuant to Section 8 (4) second sentence.

Section 24
Use of data stored in the identity card register

(1) Identity card authorities may collect, transmit, otherwise process or use personal data only in accordance with this or other Acts or statutory instruments.
(2) Identity card authorities may transmit data in the identity card register to other authorities at their request if

1. the requesting authority is authorized by law or statutory instrument to receive such data,

2. the requesting authority would not be able to fulfil its assigned duties without knowledge of the data, and

3. the data cannot be obtained from the data subject without unreasonable effort, or the nature of the task for which the data are required means that the data cannot be collected in this way.

With regard to data which are also kept in the civil register, the restrictions contained in the legislation on registration must be respected.
(3) The requesting authority shall be responsible for ensuring that the conditions in subsection 2 are met. Only those staff who are specially authorized by the head of the authority may submit requests pursuant to subsection 2. The requesting authority shall keep a record of the reason for the request and the source of the data and files transmitted. If the Federal Office for the Protection of the Constitution, the state offices for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service, the Federal Criminal Police Office or the Federal Public Prosecutor requests the identity card authority to transmit data, the requesting authority shall record the family and given name and address of the data subject and the reason for the transmission of data. Such records shall be retained separately, secured using technical and organizational means and destroyed at the end of the calendar year following the year in which the data were transmitted.
(4) Data from the identity card register may be used to correct data in the civil register and vice versa.

Section 25
Electronic data transmission and automated retrieval of photographs

(1) In the cases covered by Section 24 (2), personal data may also be transmitted electronically. Section 12 (1) third sentence shall apply mutatis mutandis.
(2) The police and public order authorities, the state tax investigation units and the customs administration authorities may retrieve photographs using automated procedures in order to prosecute crimes and traffic offences if the identity card authority is otherwise unavailable and further delay would jeopardize the purpose of the investigation. Law enforcement agencies at the county level, to be designated by state law, shall be responsible for retrieval. The retrieving authority shall be responsible for ensuring that the conditions in subsections 1 and 2 first sentence are met. The participating authorities shall keep a record of all retrievals so that their permissibility can be checked. The records shall contain

1. family and given names and date and place of birth of the person whose photograph was retrieved,
2. the date and time of retrieval,
3. the offices involved in the retrieval,
4. the name of the persons who conducted and authorized the retrieval, and
5. the file reference.

Section 24 (3), fifth sentence shall apply mutatis mutandis.

Section 26
Other storage of personal data

(1) Application for, issuance of and handing over of identity cards may not serve as a reason to store the necessary information and biometric features anywhere but by the issuing identity card authorities pursuant to Section 7 (1) and (2) according to the provisions of Sections 23 through 25. The same shall apply to the accompanying documents necessary for issuing identity cards and to the personal storage medium.
(2) Fingerprint records stored by the identity card authority shall be erased at the latest when the identity card is handed over to the card applicant.
(3) Only the card manufacturer shall be allowed to keep a central record of all serial numbers; such a record shall be used only to keep track of the whereabouts of identity cards. It shall be unlawful for the card manufacturer to store any other personal data of the card applicant unless they are exclusively and temporarily needed for manufacturing the identity card; these data shall be subsequently erased.

(4) No nationwide database of biometric features shall be established.

Part 6
Obligations of identity card holders; invalidity and withdrawal of identity cards

Section 27
Obligations of identity card holders

(1) Identity card holders shall be obligated to do the following without delay:

1. present their identity card to the identity card authority if the card contains incorrect information;

2. surrender their old identity card to the identity card authority upon receipt of a new identity card;

3. report lost identity cards to the identity card authority and, if it is found, present it to the identity card authority;

4. inform the identity card authority of any foreign citizenship acquired; and

5. inform the identity card authority of any voluntary service in the armed forces or similar organization of a foreign country of which they are citizens.

(2) The identity card holder shall take reasonable measures to ensure the confidentiality of the PIN code. In particular, card holders should not note the PIN code on the identity card or store the PIN code together with the card. If the card holder knows that the PIN code has been disclosed to a third party, he or she should immediately change the PIN code or have the electronic identification function blocked.
(3) Identity card holders should take technical and organizational measures to ensure that the electronic identification function in accordance with Section 18 is used only in an environment considered secure in accordance with the state of the art. Card holders should use in particular those technical systems and components certified by the Federal Office for Information Security as secure for this purpose.

Section 28
Invalid identity cards

(1) An identity card shall be invalid if

1. it has been altered or does not allow the card holder's identity to be established without doubt;

2. it lacks information mandated by this Act, or the information (other than height or place of residence) is incorrect;

3. the date of expiry has passed.

(2) An identity card authority shall declare an identity card invalid if the requirements for issuing the card were not met or no longer apply.
(3) Disruptions to the function of the electronic storage and processing medium shall not affect the validity of the identity card.

Section 29
Seizure and confiscation

(1) An identity card which is invalid under Section 28 (1) or (2) may be confiscated.
(2) An identity card may be confiscated if

1. it is held by an unauthorized person, or

2. there is reason to believe the conditions for confiscation under subsection 1 have been met.

(3) Seizure and confiscation shall be confirmed in writing.

Section 30
Immediate effect

Objections, actions to rescind the order that the identity card shall not entitle the holder to leave Germany (Section 6 (7)), actions opposing the suspension of authorization (Section 21 (5)), actions opposing confiscation (Section 29 (1)) and opposing seizure of the identity card (Section 29 (2)) shall have no suspensive effect.

Part 7
Fees and expenses; fines

Section 31
Fees and expenses

(1) Fees and expenses shall be charged for official acts in accordance with this Act and with regulations based on this Act to cover the administrative costs.
(2) In order to compensate for differences in buying power, the Federal Foreign Office may reduce or add a surcharge of up to 300% on fees and expenses collected by the Federal Republic of Germany's diplomatic missions abroad for official acts pursuant to subsection 1.

Section 32
Fines

(1) Anyone shall be deemed to have committed an administrative offence who

1. does not possess an identity card in violation of Section 1 (1) first sentence, also in conjunction with subsection 2 first sentence;

2. fails to present an identity card in violation of Section 1 (1) second sentence, also in conjunction with subsection 2 first sentence;

3. fails to file the relevant application or fails to do so in time in violation of Section 9 (2) second sentence;

4. fails to provide correct information in violation of Section 9 (3) first sentence;

5. uses the electronic identification function in violation of Section 18 (2) fourth sentence;

6. saves a blocking attribute, blocking code or data in violation of Section 19 (1) no. 1 or no. 2 first clause, subsection 2, 3 or 4 first sentence;

7. uses an identity card for automated retrieval or automated storage of personal data in violation of Section 20 (2);

8. uses a serial number, blocking attribute or blocking code in violation of Section 20 (3) first sentence;

9. fails to report without delay in violation of Section 27 (1) no. 3, 4 or 5;

(2) Anyone shall be deemed to have committed an administrative offence who wilfully or negligently

1. fails to provide correct information referred to in Section 18 (4) second sentence, no. 1, 3 or 4 in violation of Section 21 (1) third sentence;

2. uses an authorization in violation of Section 21 (3) third sentence;

3. fails to report or does so incorrectly, incompletely or too late in violation of Section 21 (4); or

4. uses an authorization certificate in violation of Section 21 (6) first sentence.

(3) The administrative offence may be punished by a fine of up to three hundred thousand euros in the cases covered by subsection 1, nos. 6, 7 and 8; by a fine of up to thirty thousand euros in the cases covered by subsection 1, no. 5 and subsection 2, nos. 2, 3 and 5; and by a fine of up to five thousand euros in the remaining cases.

Section 33
Fining authorities

Administrative authorities within the meaning of Section 36 (1) no. 1 of the Act on Administrative Offences, as far as this Act is enforced by federal authorities, shall be

1. in the cases of Section 32 (1) nos. 2 and 5, the Federal Police authorities within their respective remits;

2. in the cases of Section 32 (1) nos. 6 through 8, the Federal Commissioner for Data Protection and Freedom of Information;

3. in the cases of Section 32 (1) nos. 4 and 9, the Federal Foreign Office for identity card matters abroad;

4. in the cases of Section 32 (2) nos. 1 through 4 the authority responsible for issuing authorization certificates pursuant to Section 7 (4) first sentence.

Part 8
Authority to issue statutory instruments; transitional provision

Section 34
Authorization to issue statutory instruments

The Federal Ministry of the Interior shall be authorized, by statutory instrument with the agreement of the Bundesrat and in consultation with the Federal Foreign Office,

1. to determine models of the identity card,

2. to specify details of the technical specifications for storing photographs and fingerprints and for protecting access to the data stored on the electronic storage and processing medium,

3. to specify details of procedures and technical specifications for capturing and ensuring the quality of photographs and fingerprints, as well as the sequence of fingerprints to be stored in case of a missing index finger, injured fingertip or poor-quality print, and concerning the form and details of the procedure for transmitting all identity card application data from the identity card authority to the card manufacturer,

4. to specify details of the procedure for checking pursuant to Section 12 (2) second sentence,

5. to specify details of the electronic identification function pursuant to Section 18,

6. to specify the details

   a) of the PIN code,

   b) of how card holders can block and unblock the electronic identification function, and

   c) of storing and erasing the blocking attributes and blocking code;

7. to specify the details of issuing authorizations and authorization certificates, and

8. to determine in further detail the circumstances in which fees shall be payable for official acts pursuant to this Act and the level of such fees; with regard to the reimbursement of expenses, the statutory instrument may derogate from the

Administrative Costs Act and from the Act on Fees and Expenses Charged Abroad and may permit discounts and waivers of fees and expenses.

Section 35
Transitional provision

In derogation from Section 7 (2), Section 8 (2), Section 10 (1) fourth sentence and subsection 2 second sentence, Section 23 (4) second sentence and Section 31 (2), until 31 December 2012 the identity card authority pursuant to Section 7 (1) shall be responsible for Germans whose main residence is outside Germany and who are staying temporarily in the district of that identity card authority.