Übersetzung durch den Sprachendienst des Bundesministeriums des Innern.
Translations provided by the Language Service of the Federal Ministry of the Interior.
Stand: Die Übersetzung berücksichtigt die Änderung(en) des Gesetzes durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821)
Version information: The translation includes the amendment(s) to the Act by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2821)

Act on the Federal Office for Information Security

(BSI Act - BSIG)

BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821)

Section 1
German Federal Office for Information Security

The Federation shall maintain a Federal Office for Information Security as a superior federal authority, to be overseen by the Federal Ministry of the Interior.

Section 2
Definitions

(1) Information technology as referred to in this Act shall include all technical means to process or transmit information.
(2) Security of information technology as referred to in this Act shall mean compliance with certain security standards for the availability, integrity, or confidentiality of information, by means of security precautions

1. in information technology systems, components or processes, or
2. for the use of information technology systems, components or processes.

(3) Federal communications technology as referred to in this Act shall mean information technology operated by one or more federal authorities or on behalf of one or more federal authorities and used for communication or data exchange among federal authorities or between federal authorities and third parties. Communications technology of federal courts, where these do not perform administrative tasks under public law, and of the Bundestag, the Bundesrat, the Federal President and Germany's Supreme Audit Institution shall not constitute federal communications technology, where these authorities have exclusive responsibility for its operation.
(4) Federal communications technology interfaces as referred to in this Act shall mean security-relevant gateways within federal communications technology and between this technology and the information technology of individual federal authorities, groups of federal authorities, or third parties. This shall not apply to components at the network gateways which the courts and constitutional bodies referred to in subsection 3 second sentence are responsible for operating.
(5) Harmful software as referred to in this Act shall mean software programs and other information technology routines and processes intended to use or delete data without authorization or intended to interfere with other information technology processes without authorization.

(6) Security gaps as referred to in this Act shall mean characteristics of software programs or other information technology systems which third parties can use to gain unauthorized access to other information technology systems or to interfere with the function of information technology systems.
(7) Certification as referred to in the Act shall mean the determination by a certification authority that a product, process, system, protection profile (security certification), person (personal certification) or a provider of IT security services fulfils certain requirements.
(8) Protocol data as referred to in this Act shall mean control information of an information technology protocol for transferring data which is transmitted independently of the content of communication or stored on the server involved in the communication process and which is necessary for communication between sender and recipient. Protocol data may contain traffic data in accordance with Section 3 no. 30 of the Telecommunications Act (TKG) and user data in accordance with Section 15 (1) of the Telemedia Act (TMG).
(9) Data traffic as referred to in this Act shall mean data transmitted using technical protocols. Data traffic may contain telecommunications content in accordance with Section 88 (1) of the Telecommunications Act and user data in accordance with Section 15 (1) of the Telemedia Act.

Section 3
Tasks of the Federal Office

(1) The Federal Office shall promote the security of information technology. To do so, it shall perform the following tasks:

1. prevent threats to the security of federal information technology;

2. gather and analyse information on security risks and security precautions and provide the results to other authorities as needed for them to fulfil their tasks or preserve their security interests;

3. studying security risks involved in the use of information technology, and developing security precautions, especially information technology processes and devices for information technology security (IT security products) as needed by the Federation to fulfil its tasks, including research as part of its legally mandated tasks;

4. developing criteria, procedures and tools to test and evaluate the security of information technology systems or components and to test and evaluate compliance with IT security standards;

5. testing and evaluating the security of information technology systems or components and issuing security certificates;

6. testing information technology systems and components and confirming compliance with IT security standards defined in the Federal Office's technical guidelines;

7. testing, evaluating and approving information technology systems or components to be used in processing or transmitting official confidential information in accordance with Section 4 of the Security Clearance Check Act (SÜG) in the federal area or by companies in the context of federal contracts;

8. producing key data and operating cryptography and security management systems for federal information security systems used to protect official confidentiality or in other areas at the request of the authorities concerned;

9. providing support and advice on organizational and technical security measures and carrying out technical tests to protect confidential official information in accordance with Section 4 of the Security Clearance Check Act against unauthorized access;

10. developing technical security standards for federal information technology and for the suitability of information technology contractors in special need of protection;

11. making IT security products available to federal bodies;

12. providing support for the federal bodies responsible for the security of information technology, especially where these bodies undertake advisory or supervisory tasks; support for the Federal Commissioner for Data Protection and Freedom of Information shall take priority and shall be provided in line with the autonomy granted the Federal Commissioner in carrying out his/her tasks;

13. providing support for

a) the police and prosecution authorities in carrying out their legally mandated tasks,

b) the authorities for the protection of the Constitution in analysing and evaluating information derived from surveillance of terrorist activities or from intelligence activities as authorized by federal and state law,

c) the Federal Intelligence Service in carrying out its legally mandated tasks.

This support may be provided only where necessary to prevent or investigate activities directed against the security of information technology or activities carried out using information technology. The Federal Office shall keep a record of requests for support;

14. advising and warning federal and Länder bodies as well as producers, distributors and users with regard to the security of information technology, keeping in mind the possible consequences of the lack of security precautions or of inadequate security precautions;

15. creating appropriate communications structures to recognize crises at an early stage, respond and manage crises and to coordinate efforts to protect critical information infrastructures in cooperation with private industry.

(2) The Federal Office may assist the Länder in securing their information technology upon request.

Section 4
Central clearinghouse for IT security

(1) The Federal Office shall be the central clearinghouse for cooperation among federal authorities in matters related to the security of information technology.
(2) To perform this task, the Federal Office shall

1. gather and evaluate all information necessary to prevent threats to IT security, especially information concerning security gaps, malware, successful or attempted attacks on IT security and the means used to carry out such attacks;

2. inform the federal authorities without delay about information as referred to in no. 1 concerning them and of the facts of the matter ascertained.

(3) If other federal authorities become aware of information as referred to in subsection 2 no. 1 which is significant for carrying out tasks or for the IT security of other authorities, as of 1 January 2010 these federal authorities shall inform the Federal Office of this information without delay, unless prohibited by other provisions.
(4) An exception to the reporting requirements under subsection 2 no. 2 and subsection 3 shall be made for information which may not be disclosed due to confidentiality regulations or agreements with third parties, and for information whose disclosure would conflict with the constitutional status of a member of the German Bundestag or of a constitutional body, or with the legally mandated autonomy of individual bodies.

(5) The provisions regarding the protection of personal data shall remain unaffected.
(6) With the approval of the Council of Chief Information Officers of the federal ministries, the Federal Ministry of the Interior shall issue general administrative regulations for carrying out subsection 3.

Section 5
Protection against harmful software and threats to federal communications technology

(1) In order to protect federal communications technology against threats, the Federal Office may

1. use automated processes to gather and evaluate protocol data generated by operating federal communications technology as necessary to recognize, contain or remedy disruptions to or problems with federal communications technology or attacks on federal communications technology;

2. use automated processes to evaluate data generated at interfaces of federal communications technology as needed to recognize and protect against harmful software.

Unless the following subsections permit additional uses, the automated evaluation of these data must be carried out without delay and the data must be destroyed without a trace immediately after having been checked. The limitations on use shall not apply to protocol data which contain neither personal data nor data covered by telecommunications privacy. Internal protocol data of a government authority may be gathered only with the approval of the authority concerned.
(2) Protocol data as referred to in subsection 1 first sentence no. 1 may be stored longer than specified in subsection 1 first sentence no. 1, but no longer than three months, if there are concrete indications that, if suspicion is substantiated under subsection 3 second sentence, these data could be needed to protect against threats arising from the harmful software found or to recognize and protect against other harmful software. Organizational and technical measures shall be used to ensure that data stored on the basis of this subsection are evaluated only using automated processes. The data shall be depersonalized, where this is possible using automated processes. Non-automated evaluation or use of data which allows the identification of the person to whom the data pertain shall be allowed only in accordance with the following subsections. If doing so entails repersonalizing depersonalized data, this process must be ordered by the president of the Federal Office. A record is to be kept of the decision.
(3) Use of personal data beyond the restrictions specified in subsections 1 and 2 shall be permitted only when certain facts substantiate suspicion that

1. they could contain harmful software,

2. they could have been transmitted using harmful software, or

3. they could provide information about harmful software,

and when the data must be processed in order to substantiate or dispel suspicion. If suspicion is substantiated, the further processing of personal data shall be permitted as necessary

1. to protect against harmful software,

2. to protect against threats arising from the harmful software found, or

3. to recognize and protect against other harmful software.

Harmful software may be removed or disabled. Non-automated use of data in accordance with the first and second sentences may be ordered only by a Federal Office employee who is qualified to hold judicial office.

(4) The sender and recipient of the communication shall be notified at the latest after the harmful software or the threat arising from it has been recognized and averted if the sender and recipient are known or can be identified without unreasonable investigative efforts, and if notifying them would not conflict with overriding interests of third parties. Notification shall not be necessary if the person to be notified was not significantly affected and it can be assumed that he/she has no interest in being notified. The Federal Office shall present for inspection those cases in which no notification was made to its data protection official and to another Federal Office employee who is qualified to hold judicial office. The data protection official of the Federal Office shall not be bound by any instructions in carrying out this work and may not be discriminated against as a result of performing this work (Section 4f (3) of the Federal Data Protection Act). If the Federal Office's data protection official disagrees with the decision of the Federal Office, the notification shall be made after the fact. The decision not to notify shall be documented. The documentation may be used solely for purposes of data protection monitoring. It shall be destroyed after 12 months. In the cases of subsections 5 and 6, notification shall be made by the authorities referred to in those subsections in accordance with the provisions applicable to these authorities. If these provisions do not cover notification requirements, the provisions of the Code of Criminal Procedure shall be applied accordingly.
(5) The Federal Office may transmit the personal data used in accordance with subsection 3 to the law enforcement authorities for the purpose of prosecuting a criminal offence committed using harmful software under Sections 202a, 202b, 303a or 303b of the Criminal Code. Further, the Federal Office may transmit such data

1. to the federal and Länder police in order to prevent an immediate threat to public security arising from harmful software,

2. to the Federal Office for the Protection of the Constitution to inform it of evidence indicating intelligence activities or other activities on behalf of a foreign power which constitute a security threat.

(6) In other cases, the Federal Office may transmit such data

1. to the law enforcement authorities for the purpose of prosecuting a serious criminal offence, even in a single instance, especially an offence listed in Section 100a (2) of the Code of Criminal Procedure,

2. to the federal and Länder police to avert a threat to the existence or security of the state, or to the life, limb, or liberty of an individual, or to property of substantial value, the preservation of which is in the public interest,

3. to the federal and Länder offices for the protection of the Constitution, when there are concrete indications of activities within the Federal Republic of Germany directed against the protected interests listed in Section 3 (1) of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution by means of violence or preparing to use violence.

Transmission of data in accordance with the first sentence nos. 1 and 2 shall require prior judicial approval. For the procedure under the first sentence nos. 1 and 2, the provisions of the Act on Procedures in Family Matters and in Matters of Non-Contentious Jurisdiction shall apply accordingly. The court with jurisdiction shall be the local court for the district in which the Federal Office has its headquarters. Transmission of data in accordance with the first sentence no. 3 shall require the approval of the Federal Ministry of the Interior; Sections 9 to 16 of the Act to restrict the Privacy of Correspondence, Posts and Telecommunications shall apply accordingly.
(7) All other evaluation of content beyond that specified in the previous subsections and for other purposes and all other transmission of personal data to third parties shall be prohibited.

As far as possible, technical measures are to ensure that no data relating to the core area of the private sphere are collected. Information from the core area of the private sphere or data as referred to in Section 3 (9) of the Federal Data Protection Act acquired through measures referred to in subsections 1 through 3 may not be used. Information from the core area of the private sphere shall be destroyed immediately, also in case of doubt. The fact that such information was acquired and destroyed shall be documented. The documentation may be used solely for purposes of data protection monitoring. It shall be destroyed when it is no longer needed for these purposes, but no later than at the end of the calendar year following the year of documentation. If in the framework of subsections 4 or 5, the content or circumstances of communication between persons listed in Section 53 (1) first sentence of the Code of Criminal Procedure is transmitted which is subject to these persons' right to refuse to give evidence, these data may be used as evidence in criminal proceedings only if the crime in question is subject to a custodial sentence of at least five years.
(8) Before gathering and using data, the Federal Office shall have a plan for gathering and using data and shall have this plan ready for inspection by the Federal Commissioner for Data Protection and Freedom of Information. The plan shall take into account the special protection required by government communication. The criteria used in automated processes of evaluation shall be documented. The Federal Commissioner for Data Protection and Freedom of Information shall inform the Council of Chief Information Officers of the federal ministries of the results of his/her checks in accordance with Section 24 of the Federal Data Protection Act.
(9) Each calendar year, the Federal Office shall report the following information to the Federal Commissioner for Data Protection and Freedom of Information by 30 June of the reporting year:

1. the number of cases in which data as referred to in subsection 5 first sentence, subsection 5 second sentence no. 1, or subsection 6 no. 1 were transmitted, broken down according to the individual authorization of transmission,

2. the number of times personalized data were processed in accordance with subsection 3 first sentence and suspicion was dispelled,

3. the number of cases in which the Federal Office did not notify persons affected, in accordance with subsection 4 second or third sentence.

(10) Each calendar year, the Federal Office shall report to the Committee on Internal Affairs of the German Bundestag by 30 June of the year following the reporting year on its application of this provision.

Section 6
Destruction of personal data

Where the Federal Office collects personal data in the context of exercising its authority, these data are to be destroyed without delay as soon as they have served the purpose for which they were collected or are no longer needed for possible judicial review. If destruction is delayed only for possible judicial review of measures taken under Section 5 (3), the data may be used without the consent of the person concerned only for this purpose; they are to be blocked for any other purpose. Section 5 (7) shall remain unaffected.

Section 7
Warnings

(1) To fulfil its tasks under Section 3 (1) second sentence no. 14, the Federal Office may warn the affected groups or the public of security gaps in information technology products and services and of harmful software, or recommend security measures and the use of certain security products. Before publishing warnings about these products, the makers of the products concerned shall be informed in advance, as long as doing so will not interfere with achieving the intended aim of the warning. Where security gaps or harmful software should not be made public in order to prevent their further distribution or unlawful

exploitation, or because the Federal Office is bound to confidentiality with regard to third parties, the Federal Office may use objective criteria to limit the persons to be warned; in particular, a special threat to certain facilities or the exceptional reliability of the recipient may constitute objective criteria.
(2) To fulfil its tasks under Section 3 (1) second sentence no. 14, the Federal Office may include the name of the product concerned and its manufacturer in its public warnings of security gaps in information technology products and services and of harmful software or may recommend security measures and the use of specific security products, if there are sufficient indications of threat to the security of information technology. If the published information later proves to be false or the circumstances on which it was based were misrepresented, this shall be published without delay.

Section 8
Federal Office guidelines

(1) The Federal Office may set minimum standards for ensuring the security of federal information technology. With the approval of the Council of Chief Information Officers of the federal ministries, the Federal Ministry of the Interior may issue the standards set in accordance with the first sentence in full or in part as general administrative regulations for all federal bodies. Where Federal Office security standards for interministerial networks and security requirements necessary to protect the relevant network and which are to be implemented by network users are included in a general administrative regulation, these standards shall be set with the agreement of the Council of Chief Information Officers of the federal ministries. For the courts and constitutional bodies referred to in Section 2 (3) second sentence, regulations in accordance with this subsection shall have the status of recommendations.
(2) As part of its tasks under Section 3 (1) second sentence no. 10, the Federal Office shall provide technical guidelines which the federal bodies shall take into account as a framework for developing appropriate requirements for contractors (suitability) and IT products (specifications) when conducting contract award procedures. The provisions of public procurement law and on confidentiality shall remain unaffected.
(3) IT security products provided by the Federal Office in accordance with Section 3 (1) second sentence no. 11 shall be developed by the Federal Office or after conducting contract award procedures on the basis of the relevant identification of need. IT security products developed by the Federal Office may be made available only in justified exceptional cases. The provisions of public procurement law shall remain unaffected. When the Federal Office provides IT security products, the federal authorities may request these products from the Federal Office. The Council of Chief Information Officers of the federal ministries may decide that the federal authorities shall be required to request these products from the Federal Office. In this case, other federal authorities may procure their own products only when their specific requirements make the use of other products necessary. Sentences 5 and 6 shall not apply to the courts and constitutional bodies referred to in Section 2 (3) second sentence.

Section 9
Certification

(1) The Federal Office shall be the national certification authority of the federal administration for IT security.
(2) For certain products or services, security or personal certification or certification as a provider of IT security services may be applied for at the Federal Office. Applications shall be processed in the order in which they were received; the Federal Office may deviate from this if the number and extent of applications awaiting examination prevent it from examining the applications within a reasonable period of time and issuing a certificate is in the public interest. The applicant shall provide the Federal Office with the documents and information necessary to test and evaluate the system or the components or the suitability of the person and to issue the certificate.

(3) The examination and assessment may be carried out by expert bodies recognized by the Federal Office.
(4) The security certificate shall be issued if

1. information technology systems, components, products or protection profiles meet the criteria defined by the Federal Office and

2. the Federal Ministry of the Interior has determined that issuing a certificate would not conflict with any overriding public interests, in particular security concerns of the Federal Republic of Germany.

(5) Subsection 4 shall apply to the certification of persons and providers of IT security services accordingly.
(6) Expert bodies shall be recognized as referred to in subsection 3 if

1. their subject-related and personnel resources and expert qualification and reliability of the unit responsible for conformity assessment meet the criteria set by the Federal Office and

2. the Federal Ministry of the Interior has determined that issuing a certificate would not conflict with any overriding public interests, in particular security concerns of the Federal Republic of Germany.

The Federal Office shall take the necessary measures to ensure regular checking that the recognized expert bodies continue to fulfil the conditions specified in sentence 1.
(7) The Federal Office shall recognize security certificates issued by other recognized certification authorities in the European Union if they demonstrate a level of security equivalent to that of security certificates issued by the Federal Office and the Federal Office has determined their equivalence.

Section 10
Authority to issue statutory instruments

(1) After hearing from the relevant industry associations and in agreement with the Federal Ministry of Economics and Technology, the Federal Ministry of the Interior shall specify by statutory instrument the details of the procedure for issuing security certificates and recognition under Section 9 and their contents.
(2) Fees and expenses shall be charged for official acts performed under this Act and under statutory instruments issued to enforce this Act. The fees charged shall be based on the administrative effort associated with the official acts. In agreement with the Federal Ministry of Finance, the Federal Ministry of the Interior shall determine by statutory instrument the cases subject to a fee, the scale of fees charged and expenses.

Section 11
Restriction of fundamental rights

Section 5 restricts the privacy of telecommunications (Article 10 of the Basic Law).

Section 12
Council of Chief Information Officers of the federal ministries

If the Council of Chief Information Officers of the federal ministries is dissolved, it shall be replaced by a successor organization to be designated by the Federal Government. Agreement among all the federal ministries may take the place of approval by the Council. If the Council is dissolved without replacement, agreement among all the federal ministries shall take the place of its approval.