Courtesy translation published by the Federal Office for Information Security (BSI), available at https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html.

Act on the Federal Office for Information Security (BSI Act – BSIG) - courtesy translation -

Date of issue: 14/08/2009

Full citation:

"BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) last amended by Article 1 of the Act of 23 June 2017 (Federal Law Gazette I p. 1885)"

The Act was passed by the Bundestag as Art. 1 of the Act of 14/8/2009 I 2821. It came into effect in accordance with Art. 3 first sentence of this Act on 20/8/2009.

Section 1 German Federal Office for Information Security

The Federation shall maintain a Federal Office for Information Security (Federal Office) as a superior federal authority. It is responsible for information security on a national level. It is 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 this 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.

(10) Critical infrastructures as referred to in this Act shall mean facilities, equipment or parts thereof which

1. are part of the sectors energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, and the finance and insurance industries and

2. are of high importantance to the functioning of the community since their failure or impairment would result in material shortages of supply or dangers to public safety.

The critical infrastructures as referred to in this Act are defined in detail by the legal regulation pursuant to Section 10 (1).

(11) Digital services as referred to in this Act shall mean services as defined in Article 1 (1) (b) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Official Journal L 241 of 17/9/2015, p. 1) and which

1. enable consumers or entrepreneurs as referred to in Article 4 (1) (a) and (b) of the Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC (Directive on injunctions for the protection of consumers' interests) (OJ L 165 of 18/6/2013, p. 63) to conclude purchase contracts or service contracts with entrepreneurs either on the website of these services or on the website of an entrepreneur using computing services provided by these services (online marketplaces);

2. enable users to perform searches on, in principle, all websites or on websites in a certain language based on a query regarding any topic in the form of a keyword, a group of words or any other entry which then show links which can be used to retrieve contents in line with the query (online search engines);

3. enable access to a scalable and elastic pool of commonly usable computing resources (cloud computing services),

and have not been set up to protect fundamental state functions or are being used for these.
(12) Provider of digital services as referred to in this Act shall mean any legal entity offering a digital service.

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, and to third parties as needed for them to 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 prosecution of the Constitution and the Military Counterintelligence Service in analysing and evaluating information derived from surveillance of terrorist activities or from intelligence activities as authorized by federal and state law and the Law on the Military Counterintelligence Service,

    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;

13a. upon request of the competent Länder bodies, supporting these bodies in connection with the prevention of threats to the security of information technology;
upon request of the competent Länder bodies, supporting these bodies in connection with the prevention of threats to the security of information technology;

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 the security of information technology of critical infrastructures in cooperation with private industry;

16. tasks as central body for the security of information technology with regard to the cooperation with foreign competent bodies, without prejudice to special competences of other bodies;

17. tasks in accordance with Sections 8a to 8c as central body for the security of information technology of critical infrastructures and digital services;

18. providing support in the restoration of the security or functionality of information technology systems in outstanding cases pursuant to Section 5a.

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

(3) The Federal Office may advise and support operators of critical infrastructures in securing their information technology upon their request or refer them to qualified providers of security services.

Section 4 Central clearinghouse for the federal security of information technology

(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 the security of information technology, especially information concerning security gaps, malware, successful or attempted attacks on the security of information technology 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 security of information technology 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 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. The federal authorities shall be obliged to support the Federal Office regarding the measures specified in the first sentence and, while doing so, ensure that the Federal Office has access to internal protocol data of the authorities in accordance with the first sentence no. 1 and interface data in accordance with the first sentence 1 no. 2. Protocol data of federal courts may only be gathered with their approval.

(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 and to the Military Counterintelligence Service to inform them of evidence indicating intelligence activities or other activities on behalf of a foreign power which constitute a security threat, if these activities are directed against persons, offices or facilities in the field of activity of the Federal Ministry of Defence.

3. to the Federal Intelligence Service to inform it of evidence indicating an international criminal, terrorist or state attack by means of malware or comparable information technology means with harmful effect on the confidentiality, integrity or availability of IT systems in cases with significant importance with reference to the Federal Republic of Germany.

(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 and to the Military Counterintelligence Service, 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 respectively in Section 1 (1) of the Act on the Military Counterintelligence Service by means of violence or preparing to use violence.

4. to the Federal Intelligence Service, if there are actual indications for the suspicion that someone plans, commits or has committed offences pursuant to Section 3 (1), no. 8 of the Act to restrict the Privacy of Correspondence, Posts and Telecommunications and if relevant to the foreign and security policy of the Federal Republic of Germany.

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 nos. 3 and 4 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 year following 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 5a Restoration of the security or functionality of information technology systems in outstanding cases

(1) If an impairment of the security or functionality of an information technology system of a federal body or a provider of a critical infrastructure constitutes an outstanding case, the Federal Office, upon request of the body or provider concerned, may take such measures as are required to restore the security or functionality of the information technology system concerned. Where the Federal Office takes initial measures to limit the damage and ensure emergency operation on site, no fees or expenses shall be charged for the activity of the Federal Office. Any costs arsing from the consultation of qualified third parties shall remain unaffected.

(2) An outstanding case pursuant to subsection 1 shall be given in particular, if an attack of notable technical quality is concerned or a swift restoration of the security or functionality of the information technology system concerned is of special public interest.

(3) In case of measures pursuant to subsection 1, the Federal Office may collect and process personal data or data subject to the secrecy of telecommunications, to the extent it is required and appropriate to restore the security or functionality of the information technology system concerned. The data shall be deleted immediately, once they are no longer needed to restore the security or functionality of the information technology system. If the data was provided to another authority for the fulfilment of its statutory tasks in cases of subsection 4, the Federal Office, by way of derogation from the second sentence, may continue to process the data until the support of these authorities ends. Any use for other purposes is impermissible. Section 5 (7) shall be applied accordingly. Furthermore, the regulations of the Federal Data Protection Act shall apply.

(4) The Federal Office may only pass on information received within the framework of this provision with the consent of the requester, unless the information do not allow for conclusions regarding the identity of the requester or the information can be transferred in accordance with Section 5 (5) and (6). No access to the files kept in the procedures pursuant to subsection 1 shall be granted to third parties.

(5) In case of measures pursuant to subsection 1, the Federal Office may use assistance of qualified third parties subject to the consent of the requester, if this is required for the timely or complete restoration of the security or functionality of the information technology system concerned. Any costs resulting from this shall be borne by the requester. The Federal Office may also refer the requester to qualified third parties. The Federal Office and any third parties commissioned by the requester or the Federal Office pursuant to the first sentence may transfer data to each other in cases of measures pursuant to the first paragraph and subject to the consent of the requester. Subsection 3 shall apply accordingly.

(6) Where required to restore the security or functionality of the information technology system, the Federal Office may request the manufacturer of the information technology system to cooperate in the restoration of security or functionality.

(7) In justified individual cases, the Federal Office may also become active with regard to entities other than those specified in subsection 1, if requested and an outstanding case as defined by subsection 2 is given.

(8) In case facilities or activities are subject to a permission under the German Atomic Energy Act, the competent federal regulatory authorities as well as those of the Länder pursuant to nuclear law shall be consulted in the events described in subsections 1, 4, 5 and 7, prior to any actions of the Federal Office. In case of facilities or activities which are subject to a permission under the German Atomic Energy Act, the requirements under the Atomic Energy Act shall prevail in the event of measures taken by the Federal Office pursuant to Section 5a.

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

1. warn the affected groups or the public:
   a) if security gaps in information technology products and services,
   b) of harmful software and
   c) in the event of any loss of or unauthorized access to data;
2. recommend security measures and the use of certain security products.

To fulfil its tasks under the first sentence, the Federal Office may involve third parties, if this is required for an effective warning in due time. 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 7a Examination of security in information technology

(1) To fulfil its tasks under Section 3 (1) second sentence nos. 1, 14, 17 and 18, the Federal Office may examine information technology products and systems provided on the market or intended to be provided on the market. In doing so, it may use the support of third parties, unless there are no conflicting justified interests of the manufacturer of the products and services concerned.

(2) The findings obtained from the examinations may only be used to fulfil the tasks pursuant to Section 3 (1) second sentence nos. 1, 14 and 17. The Federal Office may pass on and publish its findings insofar as this is required to fulfil these tasks. Prior to any passing on or publication, the manufacturer of the products and systems concerned shall be given an opportunity to comment subject to an appropriate period.

Section 8 Federal Office guidelines

(1) The Federal Office shall develop minimum standards for ensuring the security of federal information technology. In consultation with the Council of Chief Information Officers of the federal ministries, the Federal Ministry of the Interior may issue the standards developed in full or in part as general administrative regulations for all federal bodies. The Federal Office shall advise the federal bodies upon request on the implementation of and compliance with the minimum standards. 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 8a Security regarding the information technology of critical infrastructures

(1) Operators of critical infrastructures shall be obliged, within two years from the effective date of the statutory ordinance pursuant to Section 10 (1) at the latest, to take appropriate organisational and technical precautionary measures in order to avoid disruptions of the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are decisive for the functionality of the critical infrastructures operated by them. In so doing, the state of the art shall be observed. Organisational and technical precautionary measures shall be considered appropriate, if the required efforts are not disproportionate to the consequences of a failure or an impairment of the critical infrastructure concerned.

(2) Operators of critical infrastructures and their industry associations may suggest industry-specific security standards for compliance with the requirements according to subsection 1. Upon formal request, the Federal Office shall determine whether these are suitable for complying with the requirements according to subsection 1. The determination shall be performed

1. in consultation with the Federal Office of Civil Protection and Disaster Assistance,
2. in agreement with the competent federal regulatory authority or in consultation with the otherwise competent regulatory authority.

(3) The operators of critical infrastructures shall appropriately prove compliance with the requirements according to subsection 1 at least every two years. This evidence may be provided by means of security audits, reviews or certifications. The operators shall provide the Federal Office with the results of the audits, reviews or certifications performed including any security deficiencies identified. The Federal Office may request the provision of the documentation on which the assessment was based. In the event of security deficiencies, the Federal Office, in agreement with the competent federal regulatory authority or in consultation with the otherwise competent regulatory authority, may request remedy of the security deficiencies.

(4) The Federal Office may review compliance with the requirements pursuant to subsection 1 at the operator of critical infrastructures; when performing this review, it may make use of a qualified independent third party. The operator of critical infrastructures shall grant the Federal Office and the persons acting on its behalf access to the business and operating premises during the usual business hours for the purpose of this review and, upon request, present the possibly relevant records, papers and other documents in a suitable way, provide information and grant necessary support. With regard to the review, the Federal Office shall only charge the respective operator of critical infrastructures fees and expenses, if the Federal Office has become active by reason of indications which substantiated justified doubts as to the compliance with the requirements under subsection 1.

(5) Regarding the procedures of a security audit, review and certification according to subsection 3, the Federal Office may define requirements as to the way these are implemented, the proofs to be provided in this regard, as well as the technical and organisational requirements to be met by the auditing body after consultation with representatives of the operators concerned and trade associations concerned.

Section 8b Central body for the security of information technology of critical infrastructures

(1) The Federal Office shall be the central notification body for operators of critical infrastructures in matters related to the security of information technology.

(2) To perform this task, the Federal Office shall

1. gather and evaluate all relevant information to prevent threats to the security of information technology, in particular information concerning security gaps, malware, successful or attempted attacks on the security of information technology and the observed means used to carry out such attacks,

2. analyse their potential effects on the availability of the critical infrastructures in cooperation with the competent regulatory authorities and the Federal Office of Civil Protection and Disaster Assistance,

3. continuously update the overview of the situation on the security of information technology of the critical infrastructures and

4. immediately inform
   a) the operators of critical infrastructures of information concerning them as referred to in nos. 1 to 3,

   b) the competent regulatory authorities and otherwise competent federal authorities of the information required to fulfil their tasks under nos. 1 to 3,

   c) the competent regulatory authorities of the Länder or the authorities specified for this purpose to the Federal Office by the Länder as central contact points of the information required to fulfil their tasks under nos. 1 to 3 and

   d) the competent authorities of another Member State of the European Union of major incidents reported under subsection 4 or comparable regulations which affect this Member State.

(3) The operators of critical infrastructures shall specify a contact point for the critical infrastructures operated by them to the Federal Office within six months from the effective date of the statutory ordinance pursuant to Section 10 (1). The operators shall ensure that they are available at any time via this contact point. The Federal Office shall provide information in accordance with subsection 2 no. 4 to this contact point.

(4) Operators of critical infrastructures shall immediately report the following incidents to the Federal Office via the contact point:

1. incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes which have resulted in a failure or material impairment of the functionality of the critical infrastructures operated by them,

2. significant incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes which may result in a failure or material impairment of the functionality of the critical infrastructures operated by them.

The notification shall include information on the interference, possible cross-border effects and the technical framework, in particular the assumed or actual cause, the information technology concerned, the type of facility or equipment concerned as well as the provided critical service, and the effects of the incident on this service. The specification of the operator shall only be required, if the incident has actually resulted in a failure or an impairment of the functionality of the critical infrastructure.

(5) In addition to their contact point in accordance with subsection 3, operators of critical infrastructures which belong to the same sector may specify a common higher-level point of contact. If such point of contact was specified, information shall, as a rule, be exchanged between the contact points and the Federal Office via the common point of contact.

(6) Where necessary, the Federal Office may request the manufacturer of the information technology products and systems concerned to cooperate in the elimination or prevention of an incident pursuant to subsection 4. Sentence 1 shall apply accordingly to incidents at the premises of operators and permission holders as defined by Section 8c (3).

(7) Where personal data is collected, processed or used within the framework of this provision, any processing or use beyond the above mentioned subsections for other purposes shall be impermissible. Section 5 (7) sentences 3 to 8 shall be applied accordingly. Furthermore, the regulations of the Federal Data Protection Act shall apply.

Section 8c Special requirements regarding providers of digital services

(1) Providers of digital services shall take suitable and adequate technical and organisational measures to manage risks to the security of the network and information systems which they use to provide the digital services within the European Union. They shall take measures to prevent the effects of security incidents on digital services provided within the European Union or minimise the effects as far as possible.

(2) Measures to manage risks to the security of the network and information systems under subsection 1 first sentence shall ensure a security level of the network and information systems corresponding to the existing risk, taking into account the state of the art. In this context, the following aspects shall be considered:

1. the security of the systems and facilities,
2. the detection, analysis and containment of security incidents,
3. the business continuity management,
4. the monitoring, verification and testing,
5. the compliance with international regulations.

The required measures are defined in detail by implementing acts of the Commission under Article 16 (8) of the Directive (EU) 2016/1148.

(3) Providers of digital services shall immediately report to the Federal Office any security incident materially effecting the provision of a digital service provided by them within the European Union. The requirements which have to be met to consider a security incident material are defined in detail by implementing acts of the Commission under Article 16 (8) of the Directive (EU) 2016/1148 taking into account in particular the following parameters:

1. the number of users affected by the security incident, in particular those users requiring the service to provide their own services,
2. the duration of the security incident,
3. the geographic area affected by the security incident,
4. the extent of interruption of the provision of the service,
5. the extent of the effects on economic and social activities.

The obligation to report a security incident shall not apply, if the provider does not have sufficient access to the information required to evaluate the effect of a security incident based on the parameters indicated in the second sentence. Section 8b (3) shall apply accordingly to the content of the reports, unless otherwise provided by implementing acts of the Commission under Article 16 (9) of the Directive (EU) 2016/1148. With respect to security incidents reported under the first sentence which affect another Member State of the European Union, the Federal Office shall inform the competent authority of this Member State of these security incidents.

(4) If there are indications that a provider of digital services does not meet the requirements of subsection 1 in conjunction with the implementing acts of the Commission under Article 16 (8) of the Directive (EU) 2016/1148 and subsection 2 in conjunction with the implementing acts of the Commission under Article 16 (9) of the Directive (EU) 2016/1148, the Federal Office may request the following measures of the provider of digital services:

1. the transfer of any information required to evaluate the security of its network and information systems, including evidence on security measures taken,
2. the elimination of defects in the fulfilment of the requirements specified in subsections 1 and 2.

The indications may also result from determinations presented to the Federal Office by competent authorities of another Member State of the European Union.

(5) If the headquarters, a representative or the network and information systems of a provider of digital services are located in another Member State of the European Union, the Federal Office shall cooperate with the competent authority of this Member State in the fulfilment of the tasks under subsection 4. This cooperation may include the request for taking measures as indicated in subsection 4 first sentence nos. 1 and 2.

Section 8d Scope of application

(1) Sections 8a and 8b shall not be applied to microenterprises as defined by the Recommendation 2003/361/EC of the Commission of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124 of 20/5/2003, p. 36). Article 3 (4) of the Annex to the Recommendation shall not be applied.

(2) Section 8a shall not be applied to

1. operators of critical infrastructures, insofar as they operate a public telecommunications network or provide publicly accessible telecommunications services,
2. operators of energy supply networks or energy systems as defined by the German Energy Act of 7 July 2005 (Federal Law Gazette I p. 1970, 3621) last amended by Article 3 of the Act of 17 July 2015 (Federal Law

Gazette I p. 1324), in the respectively applicable version, insofar as they are subject to the regulations of Section 11 of the Energy Act,

3. the Gesellschaft für Telematik under Article 291a (7) second sentence of Volume V of the Social Insurance Code (Fünftes Buch Sozialgesetzbuch) and Article 291b of Volume V of the Social Insurance Code, operators of services of the telematics infrastructure with respect to the services permitted under Article 291b (1a) and (1e) of Volume V of the Social Insurance Code and operators of services, insofar as they use the telematics infrastructure for applications confirmed under Article 291b (1b) of Volume V of the Social Insurance Code,

4. permission holders under Section 7 (1) of the Atomic Energy Act in the version of announcement of 15 July 1985 (Federal Law Gazette I p. 1565) last amended by Article 2 of the Act of 17 July 2015 (Federal Law Gazette I p. 1324), in the respectively applicable version within the scope of permission and

5. other operators of critical infrastructures, where they, based on legal regulations, have to meet requirements which are comparable with the requirements under Section 8a or more stringent.

(3) Section 8b (4) shall not be applied to

1. operators of critical infrastructures, where they operate a public telecommunications network or provide publicly accessible telecommunications services,

2. operators of energy supply networks or energy systems, where they are subject to the regulations of Section 11 of the Energy Act,

3. the Gesellschaft für Telematik under Article 291a (7) second sentence of Volume V of the Social Insurance Code (Fünftes Buch Sozialgesetzbuch) and Article 291b of Volume V of the Social Insurance Code, operators of services of the telematics infrastructure with respect to the services permitted under Article 291b (1a) and (1e) of Volume V of the Social Insurance Code and operators of services, where they use the telematics infrastructure for applications confirmed under Article 291b (1b) of Volume V of the Social Insurance Code,

4. permission holders under Section 7 (1) of the Atomic Energy Act for the scope of application of permission and

5. other operators of critical infrastructures, which, based on legal regulations, have to meet requirements which are comparable with the requirements under Section 8b (4) or more stringent.

(4) Section 8c (1) to (3) shall not apply to microenterprises and small companies as defined by the Recommendation 2003/361/EC. Section 8c (3) shall not apply to providers

1. having their headquarters in another Member State of the European Union or

2. which, unless based in a Member State of the European Union, have appointed a representative in another Member State of the European Union in which the digital services are also provided.

Section 8c (4) shall only apply to providers under the second sentence, insofar as they operate network and information systems in the Federal Republic of Germany which they use to provide the digital services within the European Union.

Section 8e Request for information

(1) Upon formal request, the Federal Office may only provide third parties with information on the information obtained within the framework of Section 8a (2) and (3) and Section 8c (4) and the reports under Section 8b (4) and Section 8c (4), if interests which require protection of the operator of critical infrastructures concerned or of the provider of digital services do not conflict with it and if security interests cannot be impaired by the information provided. Access to personal data shall not be granted.

(2) Access to the files of the Federal Office in matters under Sections 8a to 8c shall only be granted, provided that the requirements of Section 29 of the Administrative Procedures Law Act (Verwaltungsverfahrensgesetz) are met, if interests which require protection of the operator of critical infrastructures concerned or of the provider of digital services do not conflict with it and if no security interests can be impaired by the access to the files.

(3) The subsections 1 and 2 shall apply accordingly to operators under Section 8d (2) and (3).

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 ordinances

(1) The Federal Ministry of the Interior shall determine by means of a statutory ordinance, which does not require the approval of the Bundesrat, after hearing representatives of the scientific community, the operators concerned and the relevant industry associations, in agreement with the Federal Ministry for Economic Affairs and Energy, the Federal Ministry of Justice and Consumer Protection, the Federal Ministry of Finance, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Transport and Digital Infrastructure, the Federal Ministry of Defence and the Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety defining the services to be considered critical because of their importance in the respective sectors with respect to Section 2 (10) first sentence no. 2 and their degree of supply to be considered important, which facilities, equipment or parts thereof shall be considered to be critical infrastructures as defined by this Act. The degree of supply to be considered important under sentence 1 shall be determined by means of industry-specific threshold values for each service to be considered critical because of its importance in the respective sector. Any access to files relating to the creation or modification of this statutory ordinance shall not be granted.

(2) After hearing the relevant industry associations and in agreement with the Federal Ministry of Economic Affairs and Energy, the Federal Ministry of the Interior shall specify by statutory ordinance, which does not require the approval of the Bundesrat, the details of the procedure for issuing security certificates and recognitions under Section 9 and their contents.

(3) Fees and expenses shall be charged for individually attributable official acts performed under this Act and under statutory ordinances issued to execute this Act. The amount of 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 ordinance, which does not require approval of the Bundesrat, the cases subject to a fee, the rates of fees charged and expenses.

(4) Insofar as the implementing acts of the Commission pursuant to Article 16 (8) and (9) of the Directive (EU) 2016/1148 do not contain any final provisions on the measures to be taken by providers of digital services under Section 8c (2) or on the parameters for evaluating the relevance of the effects of security incidents under Section 8c (3) second sentence or on the form and procedure of the reports under Section 8c (3) fourth sentence, these provisions shall be defined by the Federal Ministry of the Interior in agreement with the respectively concerned departments by means of a statutory ordinance, which does not require approval of the Bundesrat.

Section 11 Restriction of fundamental rights

Sections 5 and 5a restrict 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.

Section 13 Reporting obligations

(1) The Federal Office shall inform the Federal Ministry of the Interior of its activity.

(2) The information provided under subsection 1 shall also be used by the Federal Ministry of the Interior to inform the public of any danger to the security of information technology which shall be carried out at least once a year by means of a summarising report. Section 7 (1) sentences 3 and 4 shall be applied accordingly.

(3) The Federal Office shall provide the Commission with the following information by 9 November 2018 and afterwards every two years:

1. the national measures to identify the operators of critical infrastructures;

2. a list of the sectors specified in Annex II of the Directive (EU) 2016/1148, the services to be considered critical because of their importance pursuant to Section 2 (10) first sentence no. 2 and their degree of supply to be considered important;

3. a numerical list of the operators of the sectors specified in no. 2 which are identified in the sectors specified in Annex II of the Directive (EU) 2016/1148, including a note relating to their importance to the respective sector.

The transfer shall not contain any information which may result in the identification of individual operators. The Federal Office shall immediately transfer any information provided under sentence 1 to the Federal Ministry of the Interior, the Federal Chancellery, the Federal Ministry of Economic Affairs and Energy, the Federal Ministry of Justice and Consumer Protection, the Federal Ministry of Finance, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Traffic and Digital Infrastructure, the Federal Ministry of Defence and the Federal Ministry for the Environment, Nature Protection, Building and Nuclear Safety.

(4) As soon as it becomes known that a facility or equipment pursuant to Section 2 (10) or parts of a facility or equipment provides a service to be considered critical because of its importance in one of the sectors specified in Annex II of the Directive (EU) 2016/1148 in another Member State of the European Union, the Federal Office shall enter into consultations with the competent authority of this Member State to commonly identify the operators providing critical services in the sub-sectors specified in Annex II of the Directive (EU) 2016/1148.

(5) The Federal Office shall transfer a summarising report on the reports relating to the sectors or digital services specified in Annex II of the Directive (EU) 2016/1148 to the cooperation group under Article 11 of the Directive (EU) 2016/1148 by 9 August 2018 and afterwards annually. The report shall also include the number of reports and the type of reported security incidents as well as the measures taken. The report shall not contain any information which may result in the identification of individual reports or individual operators or providers.

Section 14 Regulations on fines

(1) It is an administrative offence to wilfully or as a result of negligence,

1. contrary to Section 8a (1) first sentence in conjunction with a statutory ordinance under Section 10 (1) first sentence, fail to take a precautionary measure specified there, to take it improperly, incompletely or not in due time,

2. contravene an enforceable order pursuant Section 8a (3) fifth sentence,

3. contrary to Section 8b (3) first sentence in conjunction with a statutory ordinance pursuant to Section 10 (1) first sentence, fail to specify a contact point or not in due time,

4. contrary to Section 8b (4) first sentence no. 2, fail to submit a report, to submit it improperly, incompletely or not in due time,

5. contrary to Section 8c (1) first sentence, fail to take a measure specified there,

6. contrary to Section 8c (3) first sentence, fail to report, to not report properly, not completely or not in due time or

7. to contravene an enforceable order under Section 8c (4)
   a) no. 1 or
   b) no. 2.

(2) In the cases of subsection 1 no. 2b, the administrative offence can be punished with a fine of up to one hundred thousand euros, in the remaining cases of subsection 1 with a fine of up to fifty thousand euros. In the cases of subsection 1 nos. 5 to 7, the administrative offence shall only be punished,if the headquarters of the provider of digital services is not located in another Member State of the European Union or, where it is not based in another Member State of the European Union, it has appointed a representative there and offers the same digital services in this Member State.

(3) The administrative authority as defined by Section 36 (1) no. 1 of the Code of Administrative Offences (Gesetz über Ordnungswidrigkeiten) shall be the Federal Office.

Section 15 Applicability of the provisions for providers of digital services

Provisions referring to providers of digital services shall be applicable as of 10 May 2018.