REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

This is a consolidated version of the BND *[Federal Intelligence Service]* Act based on the bill that the German government published on 28 June 2016 with the Gesetz zur Ausland-Ausland-Fernmeldeerklärung *[Act on Signals Intelligence Gathering in Germany of Foreigners Abroad]*. To create better transparency, Reporters Without Borders has incorporated the bill in the existing BND Act and highlighted the amendments in red. We have endeavoured to take the utmost care, but are nevertheless grateful for feedback on any errors.

[Disclaimer: This is not an official translation released by the German government. We would like to especially thank Translators Without Borders for assisting in this translation.]

Federal Intelligence Service Act (BND-Gesetz-BNDG)

Section 1 - Organization, functions and powers of the BND [German Intelligence Service]

Article 1 - Organisation and functions

(1) The BND is a higher federal authority which falls under the responsibility of the Federal Chancellery. It may not be affiliated to any police authority.
(2) To acquire intelligence about foreign countries which is important to the Federal Republic of Germany from a foreign policy and security policy standpoint, the BND gathers and analyses the information required. If within the scope of this Act, information, including personal data, are captured, the capture, processing and use of such information and data is governed by articles 2 to 15, 19 to 21 and articles 23 to 32.

Article 2 - Powers

(1) The BND is permitted to capture, process and use the information required, including personal data, in so far as such action does not contravene the relevant provisions of the Federal Data Protection Act or special regulations in such Act.

1. To protect its staff, facilities, objects and sources from intelligence activities and activities that pose a security risk;
2. To conduct security screening on people currently or who will be in future in its employ;
3. To check incoming information in order to fulfil its responsibilities and
4. information on events abroad which are important for the Federal Republic of Germany's foreign and security policies, if such information can only be obtained in this way and no other state authority is responsible for the capture thereof.

(1a) (dropped)

(2) If personal data is obtained from those concerned with their knowledge, the purpose of capturing such data must be stated. The persons concerned must be informed that the information they provide is voluntary and in the event of security screening, based on paragraph 1, no. 2, they must further be informed that they have a duty of cooperation under standard labour legislation, employment legislation for civil servants and government employees, or any other contractual obligation. Any security screening is governed by the Security Screening Act of 20 April 1994 (BGBl. I, p. 869) *[BGBL = Federal Gazette]*.

(3) The BND does not have any police powers or authority to issue powers. It may not request the police, even by way of providing mutual assistance, to pursue measures which is not authorised to implement itself.

(4) If several suitable options exist, the BND must select the one which is likely to have the least negative impact on the party concerned. A measure may not cause any disadvantage which is clearly not in relation to the outcome intended.

Article 3 - Special requests for information

Should such requests be required in individual cases to fulfil the responsibilities of the BND, as specified in article 1, paragraph 2, the BND may gather information based on articles 8 a and 8b of the Federal Constitution Protection Act. Article 8a, paragraphs 2 and 2a of the Federal Constitution Protection Act are to be applied provided that instead of the serious risks to objects of protection stated in article 3, paragraph 1 of the Federal Constitution Protection Act, serious risks exist to the areas stated in article 5, paragraph 1, sentence 3, numbers 1 to 4 of the Act on the Restriction of the Confidentiality of Post and Telecommunications. Injunctions based on article 8 a, paragraphs 2 and 2a of the Federal Constitution Protection Act may only be directed at parties for whom there are actual indications that they are involved in causing or upholding such a risk, as well as at parties specified in article 8a, paragraph 2 of the Federal Constitution Protection Act. Article 8b, paragraphs 1 to 9 of the Federal Constitution Protection Act is to be applied provided that the Federal Chancellery takes the place of the Federal Ministry of the Interior. Therefore, the basic right to telecommunications confidentiality (article 10 of the Basic Law) is restricted.

Article 4 - Further requests for information

In so far as such requests are required to fulfil the functions of the BND, based on article 1, paragraph 2, the party providing or helping to provide telecommunications services as a commercial operation, can be required, based on article 8d of the Federal Constitution Protection Act to provide information on the data captured pursuant to articles 95 and 111 of the Federal Telecommunications Act. Based on article 8d, paragraph 5 of the Federal Constitution Protection Act, compensation must be paid for the provision of the information. Pursuant to article 8d, paragraph 2 of the Federal Constitution Protection Act, the basic right to telecommunications confidentiality (article 10 of the Basic Law) is restricted.

Article 5 - Special types of data capture

To gather information, including personal data, secretly, the BND, based on article 8, paragraph 2 of the Federal Constitution Protection Act, may use means if justified reasons exist which suggest are required for the BND to fulfil its responsibilities. Articles 9, 9a and 9b of the Federal Constitution Protection Act are to be applied accordingly.

Section 2 - Gathering intelligence on foreigners abroad

Article 6 - Conditions for capturing and processing data

(1) To fulfil its responsibilities, the BND may, from Germany, use technical means to capture and process information, including personal data from telecommunications networks regarding telecommunications of foreigners who are abroad (Signals Intelligence Gathering in Germany of Foreigners Abroad), if such information is required to do as follows:

1. to identify and combat risks at an early stage to the domestic or foreign security of the Federal Republic of Germany;
2. to guarantee the Federal Republic of Germany’s capacity to act, or:

3. to gain intelligence, important from a foreign policy or security policy standpoint, on events which in terms of their type and scope are determined by the Federal Chancellery in agreement with the Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economic Affairs and Energy and the Federal Ministry for Economic Co-operation and Development.

Data may only be captured from telecommunications networks which the Federal Chancellery has previously issued an injunction.

(2) The BND may only capture content data when gathering intelligence about foreigners abroad based on search terms. Such search terms must be specified and suitable for gathering intelligence on matters stated in paragraph 1, sentence 1 and the use thereof must be in accordance with the interests of the Federal Republic of Germany from a foreign policy and security policy standpoint.

(3) Search terms which lead to capture of information regarding European Union organisations, public authorities belonging to its member states, or citizens of the European Union may only be used if necessary in order to as follows:

1. identify and combat risks pursuant to article 5, sentence 3 of the Act on the Restriction of the Confidentiality of Post and Telecommunications or:
2. to gain information in accordance with paragraph 1, sentence 1, numbers 1 to 3, insofar as only data about events outside the European Union is to be gathered which is of special relevance to the security of the Federal Republic of Germany.

Search terms which lead to specific capture of information about citizens of the European Union, may only be used above any beyond such scope, if they are required to identify and combat crimes in the sense of article 3, paragraph 1 of the Act on the Restriction of the Confidentiality of Post and Telecommunications.

(4) Any capture of data from the telecommunications traffic of German citizens, or domestic legal entities, or people resident on German territory is forbidden.

(5) Gathering of intelligence on foreigners abroad to gain competitive advantages (industrial espionage), is prohibited.

(6) Data on telecommunications traffic is stored for a maximum of six months. Articles 19 and 20 are without prejudice.

(7) The technical and organisational implementation of measures specified in paragraph 1, as well as the control responsibilities within the BND, must be established in a service regulation which governs the details of the injunction proceeding. The service regulation requires the consent of the Federal Chancellery. The Federal Chancellery will inform the Parliamentary Regulation Committee.

Article 7 - Processing and using the data captured abroad

(1) Article 6, paragraph 1, sentence 1, paragraphs 3 to 6 apply to the processing and use of the data gathered on parties from abroad that is captured by the BND.

(2) Specific capture of data on organisations belonging to the European Union, public bodies belonging to member states, or to citizens of the European Union by foreign public bodies abroad may only be ordered by the BND under the conditions specified in article 6, paragraph 3.

Article 8 - Duties of the suppliers of telecommunications services

(1) Any party providing or helping to provide telecommunications services on a commercial basis, must, by injunction, give the BND information on the details of the telecommunications carried out once the injunction has come into effect, forward messages with which said party has been entrusted to convey in the telecommunications network and to enable surveillance and recording of the telecommunications. Articles 3 and 4 are without prejudice. Article 110 of the Telecommunications Act and the legal order issued specify whether and to what extent the telecommunications company in question is to make provisions for the technical and organisational implementation of the surveillance measures.

(2) Before implementing the intended measure, the company which has been ordered to comply with paragraph 1, must immediately act as follows with regard to the people who are to carry out the measure:

1. such people must be selected;
2. they must undergo basic security screening and:
3. be told that they are prohibited from revealing any details regarding such measure based on article 17 and that any violation is punishable based on article 34. The fact that such persons have been informed of such matters must be documented.

Only persons who have been screened and instructed in accordance with sentence 1 are allowed to carry out a measure. After consent of the Federal Chancellery, the head of the BND, or a representative can, in accordance with paragraph 1, order the company concerned in writing to carry out the measure before the security screening has been completed. The companies who have been ordered to carry out the measures in accordance with paragraph 1, must ensure that the security measures in the current version have been carried out which are based on the General Administrative Regulation of the Federal Ministry of the Interior on the material and organisational protection of classified documents of 31 March 2006 (GMBl of 28 August 2006, p. 846), last amended on 26 April 2010 (GMBl of 26 April 2010, p. 846). (3) Security screening pursuant to paragraph 2, sentence 1, number 2 must be carried out in compliance with the Security Screening Act. The Federal Ministry of the Interior is responsible. If a party is entrusted with carrying out a measure on whom equivalent or superior security screening based on federal or federal state law has been carried out within the last five years, new security screening is not required.

Article 9 - Directives; Public Disclosure

(1) In accordance with Article 6 paragraph 1, directives shall be made into writing upon the request of the head of the BND or a representative. The request of the directive must include:

1. The reason and duration of the measure
2. The telecommunications network concerned
3. The company concerned, as per Article 8

(2) The head of the BND or a representative determines the content of the search terms

1. in accordance with Article 6 paragraph 3 line 1 number 1, as long as they comply with the relevant bodies of the European Union and public authorities of their member states and
2. in accordance with Article 6 paragraph 1 line 1 number 2

The Federal Chancellery is to inform of such directives in accordance with Line 1.

(3) Directives in accordance with paragraph 2 and article 6 paragraph 1 are limited to nine months at the very most. Extensions up to an extra nine months are permissible so long as the premises of that directive still stand.

(4) The Federal Chancellery will inform the Independent Regulation Committee (Unabhängiges Gremium) of directives that have been completed in accordance with Article 6 paragraph 1. The Independent Regulation Committee then reviews the necessity and lawfulness of the directive. The regulation may also be enacted without prior notification of the Independent Regulation Committee if the goal of the measure would by which be impeded or significantly hindered. In this case, the Independent Regulation Committee is to be notified immediately thereafter. Ordinances determined by the Independent Regulation Committee to be unnecessary or unlawful are to be terminated immediately.

(5) The Federal Chancellery will inform the Independent Regulation Committee of measures taken by the BND in accordance with paragraph 2, insofar as these measures relate to the governing bodies of the European Union or public authorities of their member states. Ordinances determined by the Independent Regulation Committee to be unnecessary or unlawful are to be terminated immediately. The Independent Regulation Committee is furthermore mandated to review compliance with regulations set forth under Article 6 paragraph 3 at any and all times. The regulating rights of the Parliamentary Regulation Committee remain unaffected.

Article 10 - Identification and Deletion

(1) Data gathered, in accordance with Article 6, is to be identified.

(2) If an ordinance in accordance with Article 9 paragraph 2 line 2 is annulled, data already gathered under this ordinance is thereafter to be immediately deleted.

(3) If data is gathered under the premises of Article 6 paragraph 3 or Article 9 paragraph 2, this data is to be deleted immediately. The Independent Regulation Committee is to be notified of this. If it later comes to attention that a search term is associated with regulating bodies of the European Union, public bodies of an EU-member state, or an EU-citizen, the search criteria of the collected telecommunications data is to be deleted immediately. However, a targeted acquisition in accordance with Article 6 Paragraph 3 would be permissible.

(4) If data is collected under the premises of Article 6 Paragraph 4, it is to be deleted immediately. If the data is not immediately deleted, the G-10 Commission is to notify the affected Person(s) of the collection of their data in the next commission session, as soon as,

1. It can be ruled out that the purpose of the measure is not in jeopardy and
2. If there is no overwhelming detriment foreseen to the overall wellness of the federation or of an individual state.

If the notification is not completed within 12 months after the collection of the data, the G-10 Commission may additionally delay its approval of such notification. The G-10 Commission determines the extent of this delay. Five years after the collection of data, with approval by the G-10 Commission, the notification of data collection is permanently not required if – with certainty – the conditions for notification will not reoccur in the future. As long as the personal data is available for notification or judicial review, the deletion of such data is delayed and access to it is blocked. The data may only be used to these ends.

(5) If data is collected under the premises of article 6 Paragraph 5, it is to be immediately deleted.

(6) Deletions in accordance with paragraphs 2-5 are to be logged. The log entries are exclusively to be used for the implementation of data-protection monitoring. These log entries are to be stored until the end of the second year after log entry and to be immediately deleted thereafter.

Article 11 - Protection of Basic Principles

If there are factual grounds to believe that the basic principle of right to personal privacy was violated through a measure in accordance with Article 6 only, this measure is considered unlawful. In the scope of such, violations of personal privacy through measures falling under Article 6 are forbidden from exploitation. Any records of such findings are to be deleted immediately. Both their acquisition and deletion of such are to be put on record.

Article 12 - Examinations of Pertinence

The Federal Intelligence Service may collect and analyze information, including personal data from telecommunications networks as long as it has been determined (Examination of Pertinence) that they are

1. pertinent search terms or
2. pertinent telecommunications networks

and necessary for the completion of measures that fall under Article 6.

(2) The Examination of Pertinence is to be arranged by the head of the relevant authority or corresponding representatives. It may only be arranged if there are factual indications that in the telecommunications network under scrutiny there are pertinent telecommunications being transmitted. The arrangement is to be limited to no more than six months. If cooperation with the company offering the telecommunications services is required, article 6 paragraph 1 line 2, article 8 and article 9 line 1 apply accordingly.

(3) In the scope of an examination of pertinence, the collected personal data may only used for the purposes of completing the examination of pertinence. Article 5 paragraph 7 lines 2-8 of the BSI-Law applies accordingly. The Federal Intelligence Service may save the collected personal data, as long as it is required for the completion of the examination of pertinence, The analysis is to be conducted immediately after the inquiry.

(4) Personal data for examinations of pertinence under paragraph 1 line 1 is to be immediately deleted without a trace no later than two weeks after collection. Personal data for examinations of pertinence under paragraph 1 number 2 is to be immediately deleted without a trace no later than four weeks after collection. A protocol record must be kept of the deletion process. The protocol records may only be used for the completion of data protection monitoring. The protocol records may be stored until the end of the second year after the protocol process begins, and are thereafter to be immediately deleted.

(5) Under paragraph 3 line 1, a final use of the collected personal data is only legal if there are actual indications that considerable threats to

1. the health, life, or freedom of a person or
2. the safety of the Federal Republic of Germany

can be averted through such uses.

(6) Data from ongoing measures falling under article 6 may also be used for the examination of pertinence; paragraphs 1 and 3 to 5 apply accordingly.

Article 13 - Cooperation in the Scope of Signals Intelligence Gathering in Germany of Foreigners Abroad

(1) In the scope of the Signals Intelligence Gathering in Germany of Foreigners Abroad, as long as the Federal Intelligence Service cooperates with public foreign authorities in the performance of its intelligence tasks—Information, including personal data may be collected under article 14 and exchanged under article 15.

(2) Cooperation with foreign public authorities in accordance with paragraph 1 is lawful if it

1. Serves the goals of article 6 paragraph 1 line 1 numbers 1 to 3 and
2. Fulfillment of the BND's tasks would be significantly more difficult or impossible without such cooperation.

(3) Details of cooperation are to be written in a statement of purpose between the BND and the foreign public body before cooperation efforts begin. This statement should include the following:

1. The goals of the cooperation;
2. The content of the cooperation;
3. The duration of the cooperation;
4. An agreement certifying that, in the scope of the cooperation efforts, collected data may only be used for the purpose that they were originally collected for and that these uses must adhere to basic democratic principles;
5. An agreement, after the foreign public authority has willingly accepted the request of the BND to gain permission to use the data, as well as
6. An assurance of the foreign public authority to comply with removal requests by the BND.

(4) The cooperation goals and content must be concentrated on the acquisition of information that helps

1. to recognize and counter international terror threats,
2. to recognize and counter threats of illegal narcotics and weapons sales,
3. to support the German Armed Forces and to protect the armed forces of cooperating participatory states,
4. during critical developments abroad
5. to gain knowledge about the dangers and security situation facing German citizens as well as citizens of cooperating countries abroad.
6. to gain knowledge of political, business, or military operations abroad, which entail significance in foreign and security policy or
7. in similar circumstances.

(5) The statement of purpose requires the approval of the Federal Chancellery, if the cooperation ensues with foreign public authorities of EU-member states, the European economic zone, or the NATO member states; moreover, the approval of the head of the Federal Chancellery is required. The Parliamentary Regulation Committee is to inform of any such statement of purpose.

Article 14 - Collection of Exclusively Personal Data in the scope of cooperation efforts

(1) The collection of personal data in the scope of cooperation efforts in accordance with article 13 is lawful when conducted through the BND,

1. in order to achieve the agreed upon cooperation goals,
2. if during the collection of content data search terms are used that are only oriented towards achieving the agreed upon cooperation goals.

The collection of personal data and the use of search terms must be in accordance with the foreign policy and security policy interests of the Federal Republic of Germany.

(2) Moreover, article 6 paragraph 1 line 2, paragraphs 3-7 and articles 8-12 apply as well.

(3) The Signals Intelligence Gathering in Germany of Foreigners Abroad in may only be conducted through the BND itself in accordance with article 13.

Article 15 - Automated Data Transfer; Storage; Verification

(1) Information collected in the scope of the cooperation efforts, including personal/private data, may be automatically transferred to other foreign public authorities, if

1. in advance of an automated transfer detected
    a. data falling under article 10 paragraph 3 and 4 or
    b. data, whose transfer would contradict the interests of the Federal Fepublic of Germany, is deleted and
2. the instantaneous transfer of which is absolutely necessary for reaching the cooperation goals.

(2) The transfer of the data is to be regulated. The regulation data may only be used to meet the ends of the successful completion of data protection monitoring. The regulation data is available to be used until the end of the second year after its start, and is thereafter to be immediately deleted.

(3) Compliance with the guidelines falling under paragraph 1 and article 11 will be monitored on a random basis. The monitoring shall take place under supervision of an employee of the Federal Intelligence Service (BND) who is qualified in the office of the judiciary. Provided that it is recognized that data is collected under these circumstances and was passed further along to the foreign public authority, that authority is required to delete this data. The Federal Intelligence Service will inform the Federal Chancellery of the completion of monitoring under line 1, in intervals of six months at most. Details are to be determined in regulation that has been approved by the Federal Chancellery. The Federal Chancellery will then inform the Parliamentary Regulation Committee. The Independent Regulation Committee may randomly inspect compliance with paragraph 1 and article 11 anytime. Data collected under the aforementioned search terms, in the scope of cooperation efforts with the foreign public authorities, is stored for two weeks by the BND. Articles 19 and 20 remain unaltered.

Article 16 - Independent Regulation Committee

(1) The Independent Regulation Committee consists of

1. one committee chair,
2. two presiding committee members, as well as
3. three deputy committee members.

The members of the Independent Regulation Committee as well as the deputy members of the Independent Regulation Committee are independent in their administration and their directives not subjugated. The chair and presiding committee members are judges at the federal judiciary and the further presiding committee members are federal attorneys at the federal judiciary. Two deputy committee members must be judges at the federal judiciary, and one deputy committee member must be a federal attorney at the federal judiciary.

(2) For seven-year terms, the Federal Cabinet appoints

1. (at the suggestion of the president of the Federal Judiciary) the members of the independent regulation committee, who are judges at the Federal Judiciary, including their substitutes and
2. (at the suggestion of the attorney general) the member of the independent regulation committee, who is a federal attorney at the Federal Judiciary, including their substitute.

(3) The Independent Regulation Committee is to provide the necessary personnel and resources to satisfy the completion of its tasks. The office location will be set up in the Federal Judiciary.

(4) The Independent Regulation Committee must meet every three months. It will provide its own bylaws. The Independent Regulation Committee comes to decisions through a majority vote. If for any reason one or multiple members are unable to attend, their substitute is to sit in on the meeting in their place.

(5) The counseling of the Independent Regulation Committee is secret. Its members, its substitute members, and employees of the office are bound to keep confidential anything that they become acquainted with in the scope of their duties in the committee. This also remains in place once they have left their positions with the committee. The employees of the office must also undergo a further security check with a background investigation as per article 7 paragraph 1 number 3 of the law on security checks.

(6) The Independent Regulation Committee must notify the Parliamentary Regulation Committee of its duties and actions in a maximum of six month intervals.

Article 17 - Communications Prohibitions

(1) Persons, who produce telecommunications or work with such actions may not divulge any further information about measures falling under Artcile 6 paragraph 1, as well as under Article 12 paragraph 2 line 4.

(2) If there is a request for information or provision of information falling under article 8 paragraph 1 line 1, as well as in connection with article 12 paragraph 2 line 4, these facts, the content of the request, and the provision of intelligence may not be shared if the involved persons are bound to secrecy or work on classified matters.

Article 18 - Compensation

The Federal Intelligence Service (BND) will agree (under article 8 paragraph 1 line 1 or article 12 paragraph 2 line 4) with the involved companies on the aforementioned contributions, whose amount depends on the documented actual costs.

Section 3 - Data processing

Article 19 - Storage, alteration and usage of personal data

(1) The BND may store, alter and use personal data pursuant to Article 10 of the Federal Constitution Protection Act insofar as this is necessary for the completion of its duties.

(2) The storage, alteration and usage of personal data concerning minors is only permissible under the preconditions set down in Article 11 of the Federal Constitution Protection Act if, under the circumstances of a particular case, the possibility cannot be excluded that the minor presents a danger to the health or life of German nationals or to German institutions abroad.

Article 20 - Amendment, deletion and blocking of personal data

(1) The BND must amend, delete and block the personal data stored in computer files pursuant to Article 12 of the Federal Constitution Protection Act with the proviso that the limit for testing under Article 12, para. 3, Sentence 1 of the Federal Constitution Protection Act is ten years.

(2) The BND must amend and block personal data in files pursuant to Article 13, Paragraphs 1 and 2 of the Federal Constitution Protection Act. Use of electronic files is subject to Article 13, Paragraph 4 of the Federal Constitution Protection Act with the proviso that the necessity of the electronic files for completion of duties must be checked after a maximum of ten years.

Article 21 - File directives

The BND must make a file directive, which requires the consent of the Federal Chancellery, for each automated file containing personal data pursuant to Article 14 of the Federal Constitution Protection Act. Article 14, Paras. 2 and 3 of the Federal Constitution Protection Act must be applied.

Article 22 - Informing affected parties

The BND shall provide the affected party, on request, with information on the data concerning his person stored under Article 19 in accordance with Article 15 of the Federal Constitution Protection Act. The Federal Chancellery takes the place of the Federal Ministry of the Interior, which is referred to therein.

Section 4 - Transmissions and shared files

Article 23 - Transmission of information to the BND

(1) The authorities of the Federal Republic of Germany and of the federal corporate bodies under public law may voluntarily transmit information of which they have become aware, including personal data, to the BND if there is genuine evidence that such a transmission is necessary

1. for its own security pursuant to Article 2, para. 1, no. 1 or
2. as part of its duties pursuant to Article 1, para. 2 to gather information concerning the risk areas listed in Article 5, Para. 1, Sentence 3 of the Article 10 Act

. Sentence 1, No. 2 applies to the Federal Ministry of Defence and the agencies of the Federal Armed Forces with the proviso that the transmission to the BND is necessary to complete the duties set down in Article 1, para. 2.

(2) The public prosecutors and, subject to the latter's authorisation, the police forces, authorities of the Customs Investigations Service (*Zollfahndungsdienst*) and other customs services, insofar as these observe obligations pursuant to the Federal Police Act (*Bundespolizeigesetz*), voluntarily transmit to the BND the information of which they have become aware, including personal data, if there is genuine evidence that such a transmission is necessary for the BND's own security pursuant to Article 2, para. 1, no. 1. Moreover, they may voluntarily transmit the information of which they have become aware, including personal data, in accordance with Para. 1, No. 2.

(3) The BND may request each authority to transmit the information necessary for the fulfilment of its (the BND's) duties, including personal data, and, pursuant to Article 18, para. 4 of the Federal Constitution Protection Act, check officially kept registers, insofar as this is necessary to complete its duties. Article 17, Para. 1 and Article 18, Para. 5 of the Federal Constitution Protection Act must be applied.

(3a) (repealed)

(4) Article 18, Para. 6 of the Federal Constitution Protection Act must be correspondingly applied to the transmission of personal data that has become known on the basis of a measure pursuant to Article 100a of the Code of Criminal Procedure (*Strafprozeßordnung*).

Article 24 - Transmission of information by the BND

(1) The BND may transmit information, including personal data, to domestic official agencies if this is necessary for the completion of its duties or if the recipient requires the data for important purposes of public security. The BND may only transmit information, including personal data, that has been obtained via the means in Article 5 to the agencies listed in Article 19, Paragraph 1, Sentence 1 of the Federal Constitution Protection Act under the preconditions set down therein or pursuant to Paragraph 3. The recipient may only use the data for the purpose for which it was transmitted to it, unless this is set down differently in law.

(2) Article 19, Paras. 2 to 5 of the Federal Constitution Protection Act must be correspondingly applied to the transmission of information, including personal data, to other agencies; in doing so, transmission pursuant to Paragraph 4 of this regulation is only permissible if it is necessary to maintain the foreign and security policy interests of the Federal Republic of Germany and if the Federal Chancellery has given its consent. Article 18, Para. 1a, Sentences 2 to 4 of the Federal Constitution Protection Act apply correspondingly to personal data within the meaning of Article 18, Para. 1a, Sentence 1 of the Federal Constitution Protection Act that is transmitted by the Constitution Protection Services (*Verfassungsschutz*).
(3) The BND transmits information, including personal data, to the public prosecutors, the police forces and the Military Counterintelligence Service in accordance with Article 20 of the Federal Constitution Protection Act.

Article 25 - Project-related shared files with domestic public agencies

(1) The BND may set up a shared file for the duration of a time-limited, project-related cooperation with the constitution protection authorities of the federal government and of the federal states, with the Military Counterintelligence Service (*Militärische Abschirmdienst*), the police authorities of the federal government or of the federal states, and the Customs Investigation Bureau (*Zollkriminalamt*).

The project-related cooperation is intended, in accordance with the tasks and permissions of the authorities named in Sentence 1, to enable dialogue and shared evaluation of knowledge with regard to

1. the risk areas listed in Article 5, Para. 1, Sentence 3, Nos. 1 to 3 of the Article 10 Act or
2. the risk areas listed in Article 5, Para. 1, Sentence 3, Nos. 4 to 8 of the Article 10 Act, insofar as their investigation demonstrates connections to international terrorism.

Personal data concerning the risk areas in Sentence 2 may be used by the authorities involved in the project-related cooperation by means of the shared file, as part of their permissions, provided this is necessary in this context in order to complete their duties. In the event of any further use of the personal data, the authorities involved shall be subject to the laws applicable to themselves concerning the use of data.

(2) The relevant transmission regulations apply to the entry of personal data into the shared file on behalf of the authority involved in the cooperation in accordance with the proviso that the entry is only permissible if the data may be transmitted to all authorities participating in the project-related cooperation. An instance of data entry is, furthermore, only permissible if the authority that has entered the data is also permitted to store the data in its own files. The data must be labelled.

(3) Articles 19 and 20 in conjunction with Article 6, Paragraph 2, Sentences 4 and 5 and Paragraph 3, Sentence 1 and Article 14, para. 2 of the Federal Constitution Protection Act apply correspondingly to the operation of a project-related shared file. Article 22 must be applied with the proviso that the BND issues the information in coordination with the authority that bears data protection responsibility under Sentence 1 and the participating authority checks the permissibility of the issuing of information against the provisions to which it is subject.

(4) A shared file pursuant to Paragraph 1 must be limited to a maximum of two years. The time limit may be extended twice by up to a year each time if the objective of the project-related cooperation has not been achieved at the end of the project and the file remains necessary for the achievement of the objective.

(5) The amendment, blocking and deletion of data concerning a person by the authority that has entered the data are subject to the relevant regulations concerning amendment, blocking and deletion that are applicable to that authority.

(6) For the shared file in a file directive, the BND must establish the details pursuant to Article 22 in combination with Article 14, Para. 1, Sentence 1, Nos. 1 to 7 of the Federal Constitution Protection Act as well as:

1. the legal basis of the file,
2. the type of personal files to be saved,
3. the types of personal data accessible in the file,
4. prerequisites under which personal data saved in the file is transmitted to which recipients and in which procedure,
5. in agreement with the authorities participating in the project-related cooperation, the latter's relevant organisational units which are authorised to enter and access data,
6. the immediate notification of the data-entering authority about evidence for the incorrectness of data entered by the authorities involved in the shared file and the audit and, if necessary, immediate alteration, correction or deletion of this data by the authority that entered the data,

7. the possibility of supplementary entry of data in addition to that already stored about a person by the authorities involved in the shared file,
8. the logging of the time, details of the establishment of the dataset accessed and the authority responsible for the access for each access from the shared file by the BND for purposes of data protection control, including the definition of the purpose of the log data and their deletion time limit and
9. the responsibility of the BND for compensation claims from the affected parties pursuant to Article 8 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*).

The file directive requires the consent of the Federal Chancellery and of the highest federal or state authorities responsible for specialist oversight of the cooperating authorities. The Federal Commissioner for Data Protection and Freedom of Information must be consulted before issuing a file directive. Article 6, Paragraph 2, Sentence 6 of the Federal Constitution Protection Act applies accordingly.

Article 26 - Project-related shared files with foreign public agencies

(1) The BND may maintain shared files with foreign state agencies for purposes of dialogue and shared evaluation of intelligence information and knowledge (Article 27) or participate in such files (Article 30). Each file must relate to specific risk situations or groups of persons.

(2) A cooperation within the meaning of Paragraph 1 is only permissible if

1. it is of significant foreign and security policy interest for the Federal Republic of Germany,
2. compliance with fundamental rule-of-law principles is guaranteed in the participating countries and
3. the principle of reciprocity is ensured.

(3) A cooperation within the meaning of Paragraph 1 with foreign state agencies of member states of the European Union, the European Economic Area or the North Atlantic Treaty requires the consent of the Federal Chancellery; with other foreign state agencies it requires the consent of the Federal Chancellor. The Parliamentary Regulation Committee (*Parlamentarisches Kontrollgremium*) must be informed of the cooperation.

(4) The aims of the cooperation and the details of the shared data usage must, before the start of the cooperation, be mutually set down in writing by the BND and the participating foreign state agency in a declaration of intent. In the declaration of intent, in addition to the determination of the purpose of the file, there must in particular be a statement that

1. the data may only be used for this purpose and
2. the BND reserves the right to request information concerning the usage made of the data transmitted in the shared file.

Article 27 - Operation of shared files by the BND

(1) If the BND operates a file pursuant to Article 26, Paragraph 1 as its own file, this must relate to information and knowledge for identifying and countering threats within the meaning of Article 5, Paragraph 1, Sentence 3 of the Article 10 Act. Article 14, Paragraph 2 of the Federal Constitution Protection Act applies accordingly.

(2) The amendment, blocking and deletion of data concerning a person by the participating foreign state authority are subject to the applicable national law of the foreign state agency that has entered the data in question.

Article 28 - File directive for shared files

The BND must make a file directive for each file subject to shared use with foreign state agencies that it operates itself. This must contain the following details:

1. the name of the file,
2. the purpose of the file,
3. the requirements for storage, transmission and use (affected group of persons, types of data),
4. the supply or entry, including the possibility of supplementary entry of data in addition to that already stored about a person by the foreign state agencies involved in the shared file,
5. the access authorisation,
6. the review time limits and the storage duration,
7. the logging of the time of the access and of the authority responsible for the access for each access from the shared file by the BND,
8. the legal basis of the file,
9. the foreign state agencies that are authorised to enter and access data,
10. the immediate notification of the data-entering foreign state agencies of any evidence for the incorrectness of data entered by the authorities involved in the shared file and the audit and, if necessary, immediate alteration, correction or deletion of this data by the foreign state agency that entered the data, and
11. the responsibility of the BND for compensation claims from the affected parties pursuant to Article 8 of the Federal Data Protection Act.

The file directive requires the consent of the Federal Chancellery. The Federal Commissioner for Data Protection and Freedom of Information must be consulted before issuing a file directive. The auditing competence of the Federal Commissioner for Data Protection and Freedom of Information relates only to the establishment of the file by the BND and to data entered by the latter in the shared file.

Article 29 - Entry and access to the shared files operated by the BND

(1) The entry of information, including personal data, by the BND into the shared files that it operates is only permissible if the data may be transmitted to all agencies participating in the cooperation. An instance of data entry is, furthermore, only permissible if the BND is also permitted to store the data in its own files. Personal data must be labelled.

(2) The BND may also make automatic entries. Article 15, Paragraphs 1 and 3 apply accordingly.

(3) The BND and the foreign state agencies may access the stored data directly and use it if this is necessary for the fulfilment of the purpose for which the file was set up.

(4) Entry and access must be logged. Log data may only be used for the execution of the data protection control. The log data must be stored until the end of the second calendar year following the logging, and thereafter immediately deleted.

Article 30 - Participation in shared files with foreign public agencies

Any participation by the BND in shared files set up by foreign state agencies within the meaning of Article 26, Paragraph 1 requires the consent of the Federal Chancellery. Article 29, Paragraphs 1 to 3 apply accordingly.

Article 31 - Procedural rules for transmission of information

Articles 23 to 26 of the Federal Constitution Protection Act must be applied accordingly to the transmission of information pursuant to Articles 23 and 24.

Section 5 - Shared provisions

Article 32 - Applicability of the Federal Data Protection Act

When completing the tasks of the BND, Article 3, Paras. 2 and 8, Sentence 1, Paras. 2 and 3, Articles 4b and 4c as well as Articles 10 and 13 to 20 of the Federal Data Protection Act do not apply.

Article 33 - Reporting duty

The BND shall inform the Federal Chancellery of its activity. It shall also immediately inform the federal ministries, within the scope of their responsibilities, of the knowledge gained from its activity; the transmission of personal data is also permissible to this end.

Section 6 - Penalty and fine provisions

Article 34 - Penalty provisions

A person making a communication in contravention of Article 17 shall be punished by imprisonment of up to two years.

Article 35 - Fine provisions

(1) A person's conduct shall constitute an administrative offence if he

1. contravenes an enforceable order pursuant to Article 8, Paragraph 1, Sentence 1 or Paragraph 2, Sentence 3, or
2. entrusts a person in contravention of Article 8, Paragraph 2, Sentence 2.

(2) The administrative offence may be punished with a fine of up to twenty thousand euros.

(3) The administrative authority within the meaning of Article 36, Paragraph 1, Number 1 of the Code of Administrative Offences (OWiG) is the Federal Ministry for Economic Affairs and Energy.

Section 7 - Concluding provisions

Article 36 - Transfer regulation

Measures within the meaning of Articles 6, 12 and 13 and of Articles 27 and 30 that were begun before the ... [insert: date of the entry into force of the Act pursuant to Article 5] may be continued for up to twelve months after this date.