German Laws governing
Parliamentary Control of Intelligence Activities

Imprint

Publisher:
Deutscher Bundestag
Referat PD 5
Parlamentarisches Kontrollgremium,
G10-Kommission, ZFdG-Gremium,
Gemeinsamer Ausschuss nach Art. 53 a GG
Platz der Republik 1
11011 Berlin

Bundestagsadler:
Urheber: Prof. Ludwig Gies, Bearbeitung 2008: büro uebele

© Deutscher Bundestag, Berlin 2010
Alle Rechte vorbehalten
Table of Contents
5 Introduction
6 Basic Law for the Federal Republic of Germany (extracts)
7 Act governing the Parliamentary Control of Intelligence Activities by the Federation (Control Panel Act)
12 Act Restricting the Privacy of Correspondence, Posts and Telecommunications (Article 10 Act)
56 Act on the Federal Intelligence Service (BND Act)
64 Act on the Military Counterintelligence Service (MAD Act)
Introduction

This booklet contains translations of the most significant laws concerning parliamentary oversight of intelligence activities carried out by the German federal intelligence services. These translations have been produced on behalf of the Administration of the Bundestag; in some cases they were based on older translations produced by, or on behalf of, ministries and intelligence services. The sole purpose of this booklet is to serve as a source of information. Thus, the texts should not be regarded as authentic translations by the German legislature.

Three intelligence services exist at the federal level: The Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz or BfV), the Federal Intelligence Service (Bundesnachrichtendienst or BND) and the Military Counterintelligence Service (Militärischer Abschirmdienst or MAD). The BfV and MAD are domestic intelligence services, whilst the BND gathers foreign intelligence. Their activities are mainly regulated in the Federal Act on the Protection of the Constitution, the Federal Intelligence Service Act and the Act on the Military Counterintelligence Service. These Acts also contain provisions concerning parliamentary scrutiny.

There are two bodies of the German Bundestag specialized in oversight of intelligence activities. Firstly, there is the Parliamentary Control Panel (Parlamentarisches Kontrollgremium or PKGr). It consists of members of the Bundestag and is involved in “political” oversight. Secondly, there is the G10 Commission (G10 Kommission). Its members are elected by the PKGr. The G10 Commission performs more of a judicial function, with regard to surveillance measures restricting the privacy of correspondence, posts, and telecommunications. Without its permission, no such surveillance can take place. The existence of these two bodies is anchored in the Basic Law, or Grundgesetz (the German constitution). The details of their activities are regulated in the Parliamentary Control Panel Act and the Article 10 Act. However, neither body has exclusive competence. The Bundestag and its committees (the Committee on Internal Affairs, the Defence Committee or committees of inquiry, for example) are also empowered to deal with intelligence matters.

Finally, it should be noted that there are also domestic intelligence services at the level of the federal states (Länder). These are the state offices for the...
protection of the constitution (Landesämter für Verfassungsschutz or LfV). Similar oversight bodies exist at state level to those at federal level. These issues, however, are regulated mainly by state laws.

Basic Law

- Grundgesetz für die Bundesrepublik Deutschland -

...\footnote{1}

**Article 10. [Privacy of correspondence, posts and telecommunications]**

(1) The privacy of correspondence, posts and telecommunications shall be inviolable.

(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic order or the existence or the security of the Federation or of a Federal State, the law may provide that the person affected shall not be informed of the restriction and that the recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by parliament.

...

**Article 19. [Restriction of basic rights – Legal remedies]**

(1) ... (3)

(4) Should any person’s right be violated by public authority, he may have recourse to the courts. If no other jurisdiction has been established, recourse shall be to the ordinary courts. The second sentence of paragraph (2) of Article 10 shall not be affected by this paragraph.

...

**Article 45d. Parliamentary Control Panel**

(1) The Bundestag shall appoint a Panel for the oversight of intelligence activities of the Federation.

(2) Details shall be regulated by federal law.
Act governing the Parliamentary Control of Intelligence Activities by the Federation² (Control Panel Act)

- Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz) -

Section 1. Control framework
(1) With respect to the activities of the Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service, the Federal Government shall be subject to the supervision of the Parliamentary Control Panel.

(2) The rights of the German Bundestag and its committees, and those of the Commission, pursuant to the Article 10 Act, shall remain unaffected.

Section 2. Membership
(1) At the beginning of each electoral term, the German Bundestag shall elect the members of the Parliamentary Control Panel from among its own Members.

(2) It shall determine the number of members, the composition and the working methods of the Parliamentary Control Panel.

(3) Those who obtain a majority of the votes of the Members of the German Bundestag shall be elected.

(4) If a member leaves the Bundestag or his or her parliamentary group, or if a member is appointed as a minister or parliamentary state secretary, he or she shall lose his or her membership of the Parliamentary Control Panel; Section 3(3) shall remain unaffected. A new member must be elected immediately to replace him or her; the same applies if a member leaves the Parliamentary Control Panel.

Section 3. Convening
(1) The Parliamentary Control Panel shall convene at least once every

² Act as revised on July 29, 2009 (Federal Law Gazette I, p. 2346).
three months. It shall adopt its own rules of procedure.

(2) Every member may require that the Parliamentary Control Panel be convened and be provided with information.

(3) The Parliamentary Control Panel shall also continue its activities beyond the end of an electoral term of the German Bundestag until such time as the succeeding Bundestag takes a decision pursuant to Section 2.

Section 4. Information requirement of the Federal Government

(1) The Federal Government shall provide the Parliamentary Control Panel with comprehensive information regarding the general activities of the authorities referred to in Section 1(1) above and regarding processes of special significance. At the request of the Parliamentary Control Panel, the Federal Government shall also report on other processes.

(2) The political responsibility of the Federal Government for the authorities referred to in Section 1 shall remain unaffected.

Section 5. Powers of the Control Panel – official assistance

(1) As far as its supervisory rights extend, the Parliamentary Control Panel may require the Federal Government and the authorities referred to in Section 1 to release files and other documents in official safekeeping, including originals if necessary, and to transmit data stored in data files as well as to obtain access to all official premises of the authorities referred to in Section 1.

(2) It may, after notifying the Federal Government, interview members of the intelligence services, staff and members of the Federal Government and employees of other federal authorities or obtain written information from them. The persons being questioned are obliged to provide full and truthful information.

(3) The Federal Government shall satisfy the requirements of the Parliamentary Control Panel without delay.

(4) Courts of law and public authorities are obliged to provide judicial and official assistance and in particular to produce files and transmit electronic data. In so far as personal data are involved, such data may be transmitted and used solely for the purposes of the Parliamentary Control Panel.
Section 6. Scope of the information requirement – refusal to release information

(1) The obligations of the Federal Government pursuant to Sections 4 and 5 shall extend only to information and items over which the federal intelligence services have a right of disposal.

(2) The Federal Government may refuse both to provide information under Section 4 and to satisfy requirements under Section 5(1) and may prohibit the persons referred to in Section 5(2) from releasing information in so far as such refusal or prohibition is necessary for compelling reasons of access to intelligence or for reasons relating to the protection of the personal rights of a third party or if the core of executive autonomy is affected. If the Federal Government exercises these rights, the member of the Federal Government responsible for the relevant intelligence service (Section 2(1), second sentence, of the Federal Act for the Protection of the Constitution, Section 1(1), first sentence, of the Military Counter-Intelligence Service Act and Section 1(1), first sentence, of the Federal Intelligence Service Act) shall inform the Parliamentary Control Panel of the reasons for such refusal or prohibition.

Section 7. Appointment of experts

(1) In individual cases, after consultation with the Federal Government, the Parliamentary Control Panel, acting by a two-thirds majority of its members, may appoint an expert to carry out inspections for the purpose of fulfilling its supervisory duty. The expert shall report the results of his inspections to the Parliamentary Control Panel; Sections 5, 6 and 10(1) shall apply, mutatis mutandis.

(2) The Parliamentary Control Panel, acting by a two-thirds majority of its members, may decide that a written report on the inspections is to be made to the German Bundestag. The report shall communicate the course of the procedure, the discovered facts and the results of the inspections. Section 10 shall apply, mutatis mutandis.

(3) The report may also contain personal data, in so far as this is required for a retraceable account of the inspection and its results and in so far as either the persons affected have consented to publication of the data or the public interest in disclosure of the data outweighs the interests of the said persons.
Section 8. Submissions

(1) Members of the intelligence services are permitted to make submissions direct to the Parliamentary Control Panel without going through official channels in connection with official business but not in their own interests or for the needs of other members of those authorities. The submissions shall be simultaneously addressed to the head of the relevant service. The Parliamentary Control Panel shall transmit the submissions to the Federal Government for its opinion.

(2) Submissions addressed by citizens to the German Bundestag on conduct of the authorities referred to in Section 1(1) which affects them may be forwarded to the Parliamentary Control Panel for information.

Section 9. Consultation

(1) The Chairperson, his or her deputy and an authorised member may take part, in an advisory capacity, in the meetings of the Confidential Committee established by Section 10a of the Federal Budget Code. Likewise, the Chairperson of the Confidential Committee, his or her deputy and an authorised member may also take part in the meetings of the Parliamentary Control Panel in an advisory capacity.

(2) Draft copies of the annual economic plans of the services shall be transmitted to the Parliamentary Control Panel for consultation purposes. The Federal Government shall provide the Panel with information regarding the implementation of the economic plans during the budgetary year. During discussions relating to the services' economic plans and their implementation, the members of both authorities may take part in each other's meetings in an advisory capacity.

Section 10. Secret deliberations – assessments – dissenting opinions

(1) The deliberations of the Parliamentary Control Panel shall be secret. Members of the Panel, and those members of the Confidential Committee established by Section 10a of the Federal Budget Code who take part in meetings, are obliged to maintain the secrecy of matters which have come to their knowledge as a result of their activities in the Parliamentary Control Panel. This shall continue to apply after they have left both bodies. The same shall apply to matters which come to the knowledge of members of the Panel as a result of their
participation in meetings of the Confidential Committee established by Section 10a of the Federal Budget Code.

(2) Paragraph 1 above shall not apply to the assessment of certain processes if a two-thirds majority of the members of the Parliamentary Control Panel in attendance give their prior consent. In such cases, each individual member of the Panel is permitted to publish a divergent assessment (dissenting opinion).

(3) Where the Panel’s assessment or the delivery of dissenting opinions requires a presentation of the facts, the need to protect official secrets must be respected.

Section 11. Assistance of members by their own staff

(1) Members of the Parliamentary Control Panel are entitled to appoint staff of their parliamentary group to assist them in their work after consulting the Federal Government, subject to the approval of the Control Panel. The prerequisite for this activity is that such staff are authorised to deal with classified material and are formally sworn to secrecy.

(2) The appointed staff are authorised to have sight of the files and electronic data obtained by the Panel and to discuss subjects of deliberation of the Parliamentary Control Panel with members of the Panel. As a rule, they do not have access to the meetings of the Control Panel. In individual cases, the Panel may decide by a two-thirds majority of its members that staff of the parliamentary groups may attend particular meetings. Section 10(1) shall apply, mutatis mutandis.

Section 12. Human and material resourcing of the Control Panel

(1) The requisite number of employees of the Bundestag Administration shall be assigned to the Parliamentary Control Panel for its assistance. The human and material resources to be made available for this purpose shall be posted separately in the departmental budget of the German Bundestag. Section 10(1) and Section 11(1), second sentence, shall apply, mutatis mutandis, to these employees.

(2) The employees shall be given their orders in individual cases by means of instructions from the Panel and – in organisational matters and urgent cases – from the Chairperson.

(3) Subject to these instructions, employees shall be provided with in-
formation in answer to their questions and with access to the necessary files and electronic data in accordance with Section 5. Section 6(2) shall apply, mutatis mutandis.

**Section 13. Reporting**
Halfway through and at the end of each electoral term at least, the Parliamentary Control Panel shall report to the German Bundestag on its preceding supervisory activities. In these reports it shall also express its opinion as to whether the Federal Government has fulfilled its obligations to the Panel, particularly its obligation to provide information on especially important processes.

**Section 14. Jurisdiction**
The Federal Constitutional Court shall rule on disputes between the Parliamentary Control Panel and the Federal Government on the application of the Federal Government or of at least two thirds of the members of the Parliamentary Control Panel.

**Act Restricting the Privacy of Correspondence, Posts and Telecommunications**

- Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz, G10) -

**Part 1 General provisions**

**Section 1. Scope of the Act**
(1) 1. The authorities of the Federation and the Federal States for the protection of the constitution, the Military Counter-Intelligence Service and the Federal Intelligence Service charged with averting imminent danger to the free and democratic basic order or the existence or security of the Federation or of one of its constituent states, including the security of troops from the non-German Member States of the North Atlantic Treaty that are stationed in the Federal Republic of Germany

---

2. and the Federal Intelligence Service in discharging its duties pursuant to Section 1 (2) of the Act on the Federal Intelligence Service, also for the purposes defined in Section 5 (1), sentence 3, nos. 2 to 6 and Art. 8 (1), sentence 1, shall be authorized to monitor and record telecommunications and, in cases pursuant to no. 1, to open and inspect consignments subject to the privacy of correspondence or posts.

(2) Measures pursuant to sub-paragraph 1 which are carried out by authorities of the Federation shall be subject to monitoring by the Parliamentary Control Panel and by a special commission (G10 Commission).

Section 2. Obligations of providers of postal and telecommunication services

(1) Where so ordered, providers of commercial postal services or parties involved in the provision of such services shall provide the authorized agency with detailed information relating to posts and must submit to the latter consignments entrusted to them for the purposes of collection, forwarding or delivery. On request, parties subject to the obligation pursuant to sentence 1 shall furnish the authorized agency with the information on post office boxes which is necessary in preparing an order, without a separate order being required for this purpose. Where so ordered, providers of commercial telecommunications services or parties involved in the provision of such services shall provide the authorized agency with detailed information regarding telecommunications effected after the order becomes effective, submit to the latter consignments entrusted to them for transmission using telecommunication facilities and enable the monitoring and recording of telecommunications. Section 8a (2), sentence 1, nos. 3 and 4 of the Federal Act on the Protection of the Constitution, Section 4a of the Military Counterintelligence Service Act and Section 2a of the Federal Intelligence Service Act shall remain unaffected. Whether and to what extent parties subject to the obligation pursuant to sentence 3 shall be required to undertake provisions for the technical and organizational implementation of monitoring measures shall be determined in accordance with Article 110 of the Telecommunications Act and the appur-
(2) Prior to undertaking an intended restrictive measure, parties subject to the obligations pursuant to sub-paragraph 1, sentence 1 or 3 are to ensure forthwith that persons who are to be entrusted with undertaking the measure
1. are duly selected,
2. undergo a simple security check and
3. are instructed as to the prohibition of disclosure pursuant to Section 17 and the penalty for violations pursuant to Section 18; a written record is to be kept of such instruction.

Only persons who have been vetted pursuant to sentence 1 and duly instructed may be entrusted with carrying out a restrictive measure.

Subject to the consent of the Federal Ministry of the Interior, the head or deputy of the authorized agency may submit a written request to the parties subject to obligations pursuant to sub-section 1, sentence 1 or 3 to undertake the restrictive measure prior to completion of the security check. Parties subject to the obligations pursuant to sub-paragraph 1, sentence 1 or 3 are to ensure that the security measures pursuant to sub-paragraphs 1.1 to 1.4, 1.6, 2.1 and 2.3 to 2.5 of Annex 7 to the General Administrative Regulation on Physical and Organizational Protection of Classified Documents of 29 April 1994 (Joint Ministerial Gazette, p. 674) are duly undertaken.

(3) The security check pursuant to sub-paragraph 2, sentence 1, no. 1 shall be carried out in accordance with the Security Screening Act. This shall not apply to restrictive measures by an authority of a Federal State when legislation of the Federal State concerned contains comparable provisions; in this case, the legislation of the Federal State concerned shall be applicable. The Federal Ministry of the Interior shall be competent for restrictive measures by authorities of the Federation; in other cases the competence shall lie with the authorities designated under the laws of the Federal States. If a person who is to be entrusted with carrying out a restrictive measure has already been subject to a security check of an equivalent or higher category under Federal or State law within the last five years, no new security check shall be required.
Part 2 Restrictions in individual cases

Section 3. Conditions

(1) Restrictions may be ordered pursuant to Section 1 (1) no. 1 under the conditions set out therein where concrete indications give rise to the suspicion that a person is planning, committing or has committed
1. crimes against peace or of high treason (Sections 80 to 83 of the Criminal Code),
2. crimes endangering the democratic rule of law (Sections 84 to 86, 87 to 89 of the Criminal Code, Section 20 (1), nos. 1 to 4 of the Act Governing Private Associations),
3. crimes of treason or those which endanger external security (Sections 94 to 96, 97a to 100a of the Criminal Code),
4. crimes against the national defence (Sections 109e to 109g of the Criminal Code),
5. crimes against the security of troops from the non-German Member States of the North Atlantic Treaty that are stationed in the Federal Republic of Germany (Sections 87, 89, 94 to 96, 98 to 100, 109e to 109g of the Criminal Code in conjunction with Article 7 of the Fourth Criminal Law Amendment Act of 11 June 1957 (Federal Law Gazette I, p. 597) as amended by the Act of 25 June 1968 (Federal Law Gazette I, p. 741),
6. crimes under
   a) Sections 129a to 130 of the Criminal Code and
   b) Sections 211, 212, 239a, 239b, 306 to 306c, 308 (1) to (3), Section 315 (3), Section 316b (3) and Section 316c (1) and (3) of the Criminal Code which are directed against the free and democratic basic order, the existence or security of the Federation or one of its constituent states, or
7. crimes under Section 95 (1), no. 8 of the Residence Act.
The same shall apply where concrete indications give rise to the suspicion that a person is a member of an organization whose purpose or activities focus on committing criminal offences directed against the free and democratic basic order, or the existence or security of the Federation or one of its constituent states.

(1a) Subject to the conditions stipulated for the Federal Intelligence Ser-
vice in Section 1 (1), no. 1, restrictions pursuant to the aforesaid section may also be ordered for telecommunications connections on board German ships outside of German territorial waters where concrete indications give rise to the suspicion that a person is planning, committing or has committed one of the offences specified in Section 23a (1) and (3) of the Customs Investigation Service Act.

(2) An order shall be permissible only where the use of another method to investigate the facts would be futile or render their investigation significantly more difficult. Such an order may be issued only against the suspect or persons who may reasonably be assumed to be receiving or forwarding communications destined for or emanating from the suspect or whose telecommunications connection the suspect may be reasonably assumed to be using. Measures relating to consignments shall be permissible only for such consignments which may reasonably be assumed to emanate from or be destined for the party against whom the order has been issued. Post from members of the German Bundestag and the parliaments of the Federal States may not be included in a measure directed against a third party.

**Section 3a. Protection of the core area of the private sphere**

Restrictions pursuant to Section 1 (1), no. 1 shall not be permissible where concrete indications justify the assumption that information from the core area of the private sphere would be acquired solely as a result of such restrictions. Where, in the context of restrictions pursuant to Section 1 (1), no. 1, information is acquired directly, in addition to automated recording, the measure shall be interrupted immediately if concrete indications emerge during monitoring that informational content attributable to the core area of the private sphere is being disclosed. Where doubts apply in this connection, only automated recording may be continued. Automated recordings pursuant to sentence 3 shall be submitted forthwith to a specific member of the G10 commission or their deputy for a decision as to whether the data are to be used or erased. Further details shall be regulated by the rules of procedure. A decision by the member of the Commission to the effect that data may be used shall be confirmed forthwith by the Commission. A measure which has been interrupted pursuant to sentence 2
and which is not inadmissible pursuant to sentence 1 may be resumed. Information from the core area of the private sphere which has been obtained via a restriction pursuant to Section 1 (1), no. 1 may not be used. Appurtenant recordings shall be erased forthwith. Acquisition and erasure of the data shall be documented. The documentation may only be used for purposes of monitoring data protection. It shall be erased when it is no longer required for such purposes, but no later than at the end of the calendar year following the year in which documentation takes place.

Section 3b. Protection of persons entitled to refuse to give evidence

(1) Measures pursuant to Section 1 (1), no. 1 which are directed against a person specified in Section 53 (1), sentence 1, nos. 1, 2 or 4 of the Code of Criminal Procedure and which would be likely to reveal information which the person concerned would be entitled to refuse to disclose in accordance with their right to refuse to give evidence are inadmissible. Any information which is nevertheless obtained by such measures must not be used. Appurtenant recordings shall be erased forthwith. The acquisition and erasure of such information shall be documented. Sentences 2 to 3 shall apply mutatis mutandis where, as a result of a measure which is not directed against a person specified in Section 53 (1), sentence 1, nos. 1, 2 or 4 of the Code of Criminal Procedure, information is obtained from a person specified therein who would be entitled to refuse to disclose such information in accordance with their right to refuse to give evidence.

(2) Where a person specified in Section 53 (1), sentence 1, nos. 3 to 3b or no. 5 of the Code of Criminal Procedure is affected by a restriction to the effect that information would be likely to be obtained which such a person would be entitled to refuse to disclose in accordance with their right to refuse to give evidence, this shall receive special consideration in assessing the proportionality of such a measure, with due regard to the public interest in the duties performed by such a person and the interest in keeping secret the facts which are entrusted to or become known to said person. Where appropriate, the measure shall be omitted or, where the nature of the measure precludes its omission, it shall be restricted.
(3) Sub-sections 1 and 2 shall apply mutatis mutandis where the person specified in Section 53a of the Code of Criminal Procedure would be entitled to refuse to disclose the information concerned in accordance with their right to refuse to give evidence.

(4) Sub-sections 1 to 3 shall not apply where the person entitled to refuse to give evidence is a suspect within the meaning of Section 3 (2), sentence 2 or where concrete indications justify the suspicion that the person is deliberately supporting a suspect’s activities by receiving or passing on communications.

Section 4. Verification, identification and erasure obligations, transfers of data, restrictions on use of data

(1) The agency collecting data shall verify forthwith and at subsequent intervals of no more than six months whether the collected personal data are necessary in connection with its duties alone or in conjunction with previously available data for the purposes specified in Section 1 (1), no. 1. Where the data are not necessary for these purposes and are not required for transfer to other agencies, they are to be erased forthwith under the supervision of a member of staff who is qualified to hold judicial office. A record is to be kept of the erasure. The data in such records may only be used for monitoring data protection. The data in such records shall be erased at the end of the calendar year following their entry in the records. The data shall not be erased if they may be of significance in connection with a communication pursuant to Section 12 (1) or with a judicial review of the legitimacy of the restrictive measure. In this case the data are to be blocked; they may be used for these purposes only.

(2) The remaining data are to be identified accordingly. Following transfer, the recipient shall retain such identification. The data may be used only for the purposes stated in Section 1 (1), no. 1 and in subsection 4.

(3) The head or deputy head of an authority may waive the requirement for identification, where doing so is necessary to avoid jeopardizing the secrecy of a restrictive measure and where the G10 Commission or, in cases concerning transfer by an authority of a Federal State, where the competent agency under the law of this State has provided
its approval. In cases of imminent danger, the requirement for identification may be waived prior to obtaining approval. If approval is refused, the recipient of the transferred data shall provide the identification forthwith; the transferring authority shall notify the recipient accordingly.

(4) The data may be transferred only
1. to prevent or investigate criminal offences where
   a) concrete indications give rise to the suspicion that a person is planning or committing one of the offences stated in Section 3 (1) and 1a,
   b) certain facts give rise to the suspicion that a person is planning or committing another offence as stated in Section 7 (4), sentence 1,
2. in the prosecution of offences, where certain facts give rise to the suspicion that a person is committing or has committed an offence stated in no. 1, or
3. to prepare and conduct proceedings pursuant to Article 21 (2), sentence 2 of the Basic Law or a measure pursuant to Section 3 (1), sentence 1 of the Act Governing Private Associations, as necessary for the recipient to discharge its tasks.

(5) Where personal data, the transfer of which is permissible, are connected within files to other data pertaining to the data subject or a third party such that separation is not possible or would entail unreasonable effort and/or costs, transfer of these data shall also be permissible; use of these data shall not be permissible. The question as to whether the data are to be transferred shall be decided by a staff member of the transferring agency who is qualified to hold judicial office. A record is to be kept of the transfer.

(6) The recipient may use the transferred data only for the purposes for which they have been transferred. The recipient shall verify forthwith and at subsequent intervals of no more than six months whether the transferred data are necessary for these purposes. Sub-section 1, sentences 2 and 3 shall apply mutatis mutandis. The recipient shall notify the transferring agency forthwith of erasure of the data.
Part 3 Strategic restrictions

Section 5. Conditions

(1) At the request of the Federal Intelligence Service, restrictions pursuant to Section 1 may be ordered for international telecommunications traffic which is transmitted in bundled form. The telecommunications traffic concerned shall be stipulated by the federal ministry which is competent in accordance with Section 10 (1), with the approval of the Parliamentary Control Panel. Restrictions pursuant to sentence 1 shall be permissible only for the purpose of gathering information on matters, a knowledge of which is necessary in order to identify in good time the risk
1. of an armed attack on the Federal Republic of Germany,
2. of international terrorist attacks with a direct connection to the Federal Republic of Germany,
3. of the international proliferation of military weapons within the meaning of the War Weapons Control Act and of illegal foreign trade in goods, data-processing programmes and technologies in cases of substantial importance,
4. of the illegal introduction of narcotics by professional organisations or organised gangs into the territory of the European Union in cases of substantial importance relating to the Federal Republic of Germany,
5. of monetary stability in the euro currency region being undermined by counterfeiting carried out abroad or
6. of internationally organized money laundering in cases of substantial importance or
7. of the illegal smuggling of foreign persons into the territory of the European Union by professional organisations or organised gangs in cases of substantial importance relating to the Federal Republic of Germany
   a) in case of a direct link to the areas of danger specified in nos. 1 to 3 or
   b) in cases involving a substantial number of smuggled persons, in particular when a risk to the life or limb of the smuggled persons is to be assumed on account of the nature of the
smuggling operation, or

c) in cases of direct or indirect support or toleration by foreign public bodies

and to take action against such a risk. In cases pursuant to sentence 3, no. 1, restrictions may also be ordered for postal traffic; sentence 2 shall apply mutatis mutandis.

(2) In the case of restrictions on telecommunications traffic, the Federal Intelligence Service may only use search strings which serve to clarify matters relating to the area of danger specified in the order. No search strings may be used which

1. contain identifying features which will lead to the specific targeting of certain telecommunications connections or
2. apply to the core area of the private sphere.

This shall not apply to telecommunication connections abroad where the targeting of connections owned or regularly used by German nationals can be ruled out. A record is to be kept of implementation of the restrictive measures. The data in such records may be used only for purposes of monitoring data protection. They are to be erased at the end of the calendar year following their entry in the records.

Section 5a. Protection of the core area of the private sphere

No communicative content from the core area of the private sphere may be recorded as a result of restrictions pursuant to Section 1 (1), no. 2. Any communicative content from the core area of the private sphere which is recorded as a result of a restriction pursuant to Section 1 (1), no. 2 may not be used. Such content shall be erased forthwith under the supervision of a member of staff who is qualified to hold judicial office. Section 3a, sentences 2 to 7 shall apply mutatis mutandis. Acquisition and erasure of the data shall be documented. The data in such records may only be used for monitoring data protection. They shall be erased when they are no longer required for such purposes, but no later than at the end of the calendar year following the year in which documentation takes place.

Section 6. Verification, identification and erasure obligations, restrictions on use of data

(1) The Federal Intelligence Service shall verify forthwith and at subse-
quent intervals of no more than six months whether the collected personal data are necessary in connection with its duties alone or in conjunction with previously available data for the purposes specified in Section 5 (1), sentence 3. Where the data are not necessary for these purposes and are not required for transfer to other agencies, they are to be erased forthwith under the supervision of a member of staff who is qualified to hold judicial office. A record is to be kept of the erasure. The data in such records may only be used for monitoring data protection. The data in such records shall be erased at the end of the calendar year following their entry in the records. Except in cases of initial checking pursuant to sentence 1, the data shall not be erased if they may be of significance in connection with a communication pursuant to Section 12 (2) or with a judicial review of the legitimacy of the restrictive measure. In this case the data are to be blocked; they may be used for these purposes only.

(2) The remaining data are to be identified accordingly. Following transfer, the identification is to be maintained by the recipient. The data may be used only for the purposes stated in Section 5 (1), sentence 3 and for transfers pursuant to Section 7 (1) to (4) and Section 7a.

(3) On request from the Federal Intelligence Service, in order to assess the relevance of recorded telecommunications the collected data may, by order of the competent federal ministry in accordance with Section 10 (1), be checked by means of an automated process against existing telephone numbers or other forms of identification for specific telecommunications connections for which there are concrete indications that they are linked to the area of danger for which the monitoring measure has been ordered. The Federal Intelligence Service may also use telephone numbers or other forms of identification for specific telecommunications connections in Germany for the purposes of such checks. The data employed for such checks must not be used as search strings as defined in Section 5 (2), sentence 1. A record shall be kept of the check and of the grounds for using the data employed for the check. The data in such records may only be used for purposes of monitoring data protection. They shall be destroyed at the end of the calendar year following their entry in the records.
Section 7. Transfer by the Federal Intelligence Service

(1) Personal data collected via restrictions pursuant to Section 5 may be transferred in accordance with Section 12 of the Act on the Federal Information Service in order to provide notification of the dangers stated in Section 5 (1), sentence 3.

(2) Personal data collected via restrictions pursuant to Section 5 may be transferred to the authorities of the Federation and the Federal States for the protection of the constitution and to the Military Counter-Intelligence Service if

1. there are concrete indications that the data are necessary in order to gather and evaluate information on activities in the Federal Republic of Germany which are aimed at subverting the vested rights stipulated in Section 3 (1), nos. 1, 3 and 4 of the Federal Act on the Protection of the Constitution through the use of violence or preparations for the use of violence, or
2. certain facts give rise to a suspicion of intelligence service activities for a foreign power or such activities posing a threat to security.

(3) Personal data collected via restrictions pursuant to Section 5 (1), sentence 1 in conjunction with sentence 3, no. 3 may be transferred to the Federal Office of Economics and Export Control (BAFA) if there are concrete indications that a knowledge of these data is necessary

1. to inform participants in foreign trade about circumstances which are of relevance to compliance with restrictions on foreign trade, or
2. in connection with a procedure for issuing an export licence or to notify participants in foreign trade, where such a procedure establishes a licence requirement for the export of goods.

(4) Personal data collected via restrictions pursuant to Section 5 may be transferred to the authorities charged with policing duties in order to prevent offences where

1. concrete indications give rise to the suspicion that a person is planning or committing
   a) offences pursuant to Section 129a of the Criminal Code, also in conjunction with Section 129b (1), and pursuant to Sections 146, 151 to 152a or Section 261 of the Criminal Code,
   b) offences pursuant to Section 34 (1) to (6) and (8), Section 35 of the Foreign Trade and Payments Act, Sections 19 to 21 or
Section 22a (1) nos. 4, 5 and 7 of the War Weapons Control Act or

c) offences pursuant to Section 29a (1), no. 2, Section 30 (1), nos. 1, 4 or Section 30a of the Narcotics Act, or

2. certain facts give rise to the suspicion that a person is planning or committing

a) offences described in Section 3 (1), sentence 1, nos. 1 to 5 and 7, (1), sentence 2 or (1a) of this Act or in Section 129a (1) of the Criminal Code, or

b) offences pursuant to Sections 130, 232 (3), (4) or (5), second clause, Sections 249 to 251, 255, 305a, 306 to 306c, 307 (1) to (3), Section 308 (1) to (4), Section 309 (1) to (5), Sections 313, 314, 315 (1), (3) or (4), Section § 315b (3), Sections 316a, 316b (1) or (3) or Section 316 c (1) to (3) of the Criminal Code, or

c) criminal offences pursuant to Section 96 (2), also in conjunction with sub-section (4), and Section 97 (1) to (3) of the Residence Act.

The data may be transferred to the competent authorities for the purpose of prosecuting offences, if certain facts give rise to the suspicion that a person is committing or has committed an offence described in sentence 1.

(5) Transfer shall be permissible only where it is necessary for discharging the recipient’s tasks. Where personal data, the transfer of which is permissible, are connected within files to other data pertaining to the data subject or a third party such that separation is not possible or would entail an unreasonable effort and/or costs, transfer of these data shall also be permissible; use of these data shall not be permissible. The question as to whether the data are to be transferred shall be decided by a member of staff of the Federal Intelligence Service who is qualified to hold judicial office. A record is to be kept of the transfer.

(6) The recipient may use the data only for the purposes for which they have been transferred. The recipient shall verify forthwith and at subsequent intervals of no more than six months whether the transferred data are necessary for these purposes. Section 4 (6), sentence 4 and Section 6 (1), sentences 2 and 3 shall apply mutatis mutandis.
Section 7a. Transfer by the Federal Intelligence Service to foreign public bodies

(1) The Federal Intelligence Service may only transfer personal data collected on the basis of restrictions pursuant to Section 5 (1), sentence 3, nos. 2, 3 and 7 to foreign public bodies charged with intelligence tasks where

1. transfer is necessary in order to safeguard foreign-policy or security interests of the Federal Republic of Germany or substantial security interests of the foreign state,

2. there are no overriding legitimate interests of the data subject which preclude such transfer, whereby in particular an appropriate standard of data protection must be ensured in the foreign state and it must be possible to rely on the recipient using the data in accordance with fundamental principles of the rule of law, and

3. the principle of reciprocity is upheld.

Transfer shall require the approval of the Federal Chancellery.

(2) Subject to the conditions stipulated in sub-section 1, the Federal Intelligence Service may also transfer personal data collected by way of restrictions pursuant to Section 5 (1), sentence 3, nos. 2, 3 and 7 to bodies of the armed forces stationed in Germany in accordance with Article 3 of the Agreement to Supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to Foreign Forces stationed in the Federal Republic of Germany of 3 August 1959 (Federal Law Gazette 1961 II, p. 1183, 1218), where such transfer is necessary in discharging the tasks within the remit of such bodies.

(3) The question as to whether the data are to be transferred shall be decided by a member of staff of the Federal Intelligence Service who is qualified to hold judicial office. A record is to be kept of the transfer. The Federal Intelligence Service shall keep a record of the purpose of transfer, the corresponding order, the file reference and the recipient of the transferred information. The records shall be kept separately, secured against unauthorised access and destroyed at the end of the calendar year following the year in which they are drawn up.

(4) The recipient shall be obligated

1. to use the transferred data only for the purpose for which they have
been transferred,
2. to maintain any identification which has been applied to the data and
3. to provide the Federal Intelligence Service with information on use of the data on request.

(5) The competent federal ministry shall inform the G10 Commission about transfers pursuant to sub-sections 1 and 2 at monthly intervals.

(6) The Parliamentary Control Panel shall be informed about transfers undertaken pursuant to sub-section 1 and 2 at intervals of six months at the most.

Section 8. Danger to the life or limb of a person abroad

(1) At the request of the Federal Intelligence Service, restrictions pursuant to Section 1 may be ordered for international telecommunications traffic within the meaning of Section 5 (1), sentence 1 where this is necessary in order to identify in good time a danger to the life or limb of a person abroad in individual cases or to counter such a danger, as a result of which interests of the Federal Republic of Germany are directly affected in a special way. Section 5 (1), sentence 2 shall apply mutatis mutandis.

(2) The telecommunications traffic concerned shall be stipulated by the federal ministry which is competent in accordance with Section 10 (1), with the approval of the Parliamentary Control Panel. Such approval shall require a majority of two thirds of the Panel’s members. The approved restriction shall lapse after two months at the latest. Renewed approval shall be permissible, provided that the attendant conditions continue to apply.

(3) An order shall be permissible only where the use of another method to investigate the facts would be futile or render their investigation significantly more difficult. The Federal Intelligence Service may only use search strings which serve to obtain information on the danger specified in the order. Section 5 (2), sentences 2 to 6 shall apply mutatis mutandis. Where the monitoring measure is necessary in an individual case in order to avert a risk to the life or limb of a person, the search strings may also contain identifying features which will lead to specific targeting of the telephone number or another form of identifi-
cation of this person's telecommunications connection abroad.

(4) The Federal Intelligence Service shall verify forthwith and at subsequent intervals of no more than six months whether the collected personal data are necessary in connection with its duties alone or in conjunction with previously available data for the purposes specified in sub-section 1. Where the data are not necessary for this purpose, they are to be erased forthwith under the supervision of a member of staff who is qualified to hold judicial office. A record is to be kept of the erasure. Section 6 (1), sentences 4 and 5, and (2), sentences 1 and 2 shall apply mutatis mutandis. The data may be used only for the purposes stated in sub-sections 1, 5 and 6.

(5) In accordance with Section 12 of the Act on the Federal Intelligence Service, the collected personal data may be transferred to provide notification of the danger stated in sub-section 1.

(6) The collected personal data may be transferred to the competent authorities in order to prevent offences where concrete indications give rise to the suspicion that a person is planning or committing an offence which might contribute to inducing or maintaining the danger described in sub-section 1. The data may be transferred to the competent authorities for the purpose of prosecuting offences, if certain facts give rise to the suspicion that a person is committing or has committed an offence described in sentence 1. Section 7 (5) and (6) and Section 7a (1) and (3) to (6) shall apply mutatis mutandis.

**Part 4 Procedures**

**Section 9. Application**

(1) Restrictive measures under this Act may be ordered only upon application.

(2) Within their respective spheres of responsibility, applications may be submitted by

1. the Federal Office for the Protection of the Constitution,
2. the authorities of the Federal States for the protection of the constitution,
3. the Military Counter-Intelligence Service Office and
4. the Federal Intelligence Service,

whereby applications are to be filed by the head of the authority con-
cerned or his deputy.

(3) The application shall be submitted in writing, stating the grounds for its submission. It must contain all the information required for the order. In cases pursuant to Sections 3 and 8, the applicant shall demonstrate that the use of another method to investigate the facts would be futile or render their investigation significantly more difficult.

Section 10. Order

(1) Where applications are submitted by the authorities for the protection of the constitution of the Federal States, the responsibility for ordering restrictive measures shall lie with the competent supreme State authority, otherwise responsibility shall lie with a federal ministry appointed by the Federal Chancellor.

(2) The order shall be issued in written form. It shall state the grounds for the order and the agency authorized to carry out the monitoring and set out the nature, scope and duration of the restrictive measure.

(3) In cases pursuant to Section 3, the order must specify the party against whom the restrictive measure is directed. In the case of monitoring of telecommunications, the order shall state the telephone number or another form of identification of the telecommunications connection or the identification code of the terminal, where this code is assigned solely to this terminal.

(4) In cases pursuant to Sections 5 and 8, the search strings are to be stated in the order. The region about which information is to be gathered and the transmission channels subject to the restriction are also to be specified. Further, the order shall specify what proportion of the transmission capacity available on these transmission paths may be monitored. In cases pursuant to Section 5, this proportion may not exceed 20 per cent.

(5) In cases pursuant to Sections 3 and 5, the order shall be valid for a maximum of three months. Extensions for further periods of not more than three months shall be permissible, provided that the conditions pertaining to the order continue to apply.

(6) Parties subject to obligations pursuant to Section 2 (1), sentence 1 or 3 are to be notified of the order where this is necessary in order to en-
able them to fulfil their obligations. No such notification shall be necessary if the order can be executed without the involvement of the said parties.

(7) The Federal Office for the Protection of the Constitution shall inform the relevant authority for the protection of the constitution of the Federal State of the restrictive orders issued within the latter’s territory. The authorities for the protection of the constitution of the Federal States shall notify the Federal Office for the Protection of the Constitution of the restrictive orders issued in their respective territories.

Section 11. Enforcement

(1) Restrictive measures resulting from the order shall be undertaken on the responsibility of the authority in response to whose application the order has been issued, under the supervision of a member of staff who is qualified to hold judicial office.

(2) The measures shall be discontinued forthwith, if they are no longer necessary or the conditions pertaining to the order no longer apply. The agency which issued the order and the party subject to obligations pursuant to Section 2 (1), sentence 1 or 3 who has been informed of the order shall be notified when the order is discontinued. Notification of the party subject to obligations shall be waived if the order has been executed without their involvement.

(3) Postal consignments which have been surrendered for opening and inspection shall be returned to the postal service forthwith. Telegrams may not be withdrawn from the postal service. The agency authorized to carry out inspection shall be furnished with a copy of the telegram concerned.

Section 12. Notification of data subjects

(1) The data subject shall be informed of restrictive measures pursuant to Section 3 after their discontinuation. Such notification shall be withheld as long as it cannot be ruled out that informing the data subject might jeopardise the purpose of the restriction or as long as any general disadvantages to the interests of the Federation or of a Federal State are foreseeable. Where such notification continues to be withheld pursuant to sentence 2 twelve months after termination of the measure, its continued deferment shall require the approval of the
G10 Commission. The G10 Commission shall determine the duration of the continued deferment. No notification shall be necessary where the G10 Commission has unanimously found that

1. one of the conditions stipulated in sentence 2 continues to apply five years after termination of the measure,
2. it is practically certain that such a condition will continue to apply in the future and
3. the conditions pertaining to erasure apply both at the collecting agency and at the receiving agency.

(2) Sub-section 1 shall apply mutatis mutandis to restrictive measures pursuant to Sections 5 and 8 where the personal data are not erased immediately. The five-year period shall begin on collection of the personal data.

(3) The obligation to notify the data subject shall lie with the authority that applied for the order. Where personal data have been transferred, notification shall be effected in consultation with the recipient.

Section 13. Recourse to courts of law
No appeal against the ordering and implementation of restrictive measures pursuant to Sections 3 and 5 (1), sentence 3, no. 1 by recourse to a court of law shall be admissible prior to notification of the data subject.

Part 5 Oversight

Section 14. Parliamentary Control Panel
(1) The federal ministry responsible under Section 10 (1) for ordering restrictive measures shall report to the Parliamentary Control Panel on implementation of this Act at intervals of no more than six months. The Panel shall furnish the German Bundestag with an annual report on the implementation, nature and scope of the measures pursuant to Sections 3, 5 and 8, observing the principles stipulated in Section 5 (1) of the Control Panel Act pertaining to the Control Panel.

(2) In cases of imminent danger, provisional approval may be granted for restrictions pursuant to Sections 5 and 8 by the chairperson of the Parliamentary Control Panel and his deputy. The subsequent approval of
the Parliamentary Control Panel is to be obtained forthwith. The provisional approval shall expire after two weeks at the latest.

Section 15. G10 Commission

(1) The G10 Commission shall comprise a chairperson qualified to hold judicial office, three associate chairpersons and four deputy members who may take part in the meetings with the right to speak and to ask questions. In the event of a tie, the chairperson shall have the deciding vote. The members of the G10 Commission shall remain independent in discharging their duties and shall not be subject to instructions. They shall hold an honorary public office and shall be appointed by the Parliamentary Control Panel after a hearing by the Federal Government for the duration of one legislative term of the German Bundestag, subject to the proviso that their term of office shall not end until the members of the Commission are newly appointed, but no later than three months after the end of the legislative term.

(2) The discussions of the G10 Commission shall be confidential. The members of the Commission shall be obliged to maintain the confidentiality of matters of which they obtain knowledge in the course of their activities in the Commission. This obligation shall continue to apply after they leave the Commission.

(3) The G10 Commission shall be provided with the personnel and material resources necessary to discharge its duties; its funding shall be shown in a separate section of the German Bundestag’s budget. The Commission shall be provided with personnel who possess technical expertise.

(4) The G10 Commission shall meet at least once a month. It shall draw up its own rules of procedure, which shall require the approval of the Parliamentary Control Panel. The Federal Government shall be heard before such approval is given.

(5) The G10 Commission shall decide ex-officio or on the basis of complaints whether restrictive measures are permissible and necessary. The Commission’s supervisory powers shall extend to the entire scope of collection, processing and use of the personal data obtained pursuant to this Act by intelligence services of the Federation, including the decision on notification of data subjects. In particular, the Commis-
sion and its staff shall be
1. provided with information in response to their questions,
2. granted the right to inspect all documentation and records, in particular stored data and data-processing programmes which pertain to the restrictive measure, and
3. granted access to all official premises at all times.
The Commission may grant the Federal Data Protection Commissioner an opportunity to deliver an opinion on matters of data protection.

(6) The competent federal ministry shall report to the G10 Commission every month on the restrictive measures which it has ordered, prior to their being enforced. In cases of imminent danger, it may also order the enforcement of restrictive measures prior to notifying the Commission. The competent federal ministry shall immediately revoke any orders which the Commission declares impermissible or unnecessary. In cases pursuant to Section 8, the order shall lapse unless confirmed by the Chairperson or his/her deputy within three days. Subsequent confirmation shall be obtained from the Commission forthwith.

(7) The competent federal ministry shall report to the G10 Commission every month on communications by federal authorities pursuant to Section 12 (1) and (2) or on grounds hindering such communications. Any communication which the Commission considers necessary shall be effected forthwith. Section 12 (3), sentence 2 shall remain unaffected where it is necessary to consult an authority of a Federal State.

Section 16. Parliamentary oversight in the Federal States
The legislature of the Federal States shall regulate the parliamentary oversight of the supreme authorities of the Federal States responsible pursuant to Section 10 (1) for ordering restrictive measures and review of the restrictive measures ordered by the latter. Personal data may be transferred to authorities of a Federal States only where the supervision of their processing and usage is regulated by the legislature of this Federal State.

Part 6 Provisions as to punishments for criminal offences and fines

Section 17. Prohibition of disclosure
(1) Where telecommunications are monitored under this Act or pursuant
Sections 100a, 100b of the Code of Criminal Procedure, this fact may not be disclosed to others by persons who provide commercial telecommunications services or are involved in the provision of such services.

(2) Where the surrender of consignments is ordered pursuant to Section 2 (1), sentence 1 or 3, this fact may not be disclosed to others by persons who are obliged to surrender such consignments or are entrusted with forwarding such consignments.

(3) Where information is requested or furnished pursuant to Section 2 (1), this fact or the contents of the request or the furnished information may not be disclosed to others by persons who are obliged to provide such information or are entrusted with or involved in providing such information.

Section 18. Criminal offences
Anyone disclosing information in violation of Section 17 shall be punishable with a prison term of up to two years or a fine.

Section 19. Administrative offences
(1) The following actions constitute administrative offences:
   1. violating an enforceable order pursuant to Section 2 (1), sentence 1 or 3,
   2. entrusting a person in violation of Section 2 (2), sentence 2 and
   3. failing to ensure that a security measure is undertaken, in violation of Section 2 (2), sentence 3.

(2) An administrative offence may be punished by a fine of up to fifteen thousand euros.

(3) The authority responsible for imposing fines pursuant to Section 36 (1), no. 1 of the Administrative Offences Act shall be the competent agency pursuant to Section 10 (1).

Part 7 Final provisions

Section 20. Remuneration
The agencies authorised under Section 1(1) shall grant remuneration for services provided under Section 2(1), the amount of which shall be
determined in accordance with Section 23 of the Judicial Remuneration and Compensation Act. In the cases referred to in Sections 5 and 8 of the present Act, agreement shall be reached on remuneration, the amount of which shall be based on actual substantiated costs.

**Section 21. Curtailment of fundamental rights**

This Act shall curtail the fundamental right of the privacy of correspondence, posts and telecommunications (Article 10 of the Basic Law).

### 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 (Federal Act on Protection of the Constitution)**4**

- Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz) -

#### PART I Cooperation, Functions of the Protection of the Constitution Agencies

**Section 1. Obligation of the Federation and the Federal States to Cooperate**

1. The protection of the constitution serves the protection of the free democratic basic order, the existence and the security of the Federation and the Federal States.

2. The Federation and the Federal States are obliged to cooperate in matters relating to the protection of the constitution.

---

Cooperation includes mutual support and assistance.

Section 2. Protection of the Constitution Agencies

(1) In order to ensure the cooperation of the Federation with the Federal States, the Federation shall maintain a Federal Office for the Protection of the Constitution as a federal superior authority subordinate to the Federal Ministry of the Interior. The Federal Office for the Protection of the Constitution shall not be affiliated to a police organ.

(2) In order to ensure the cooperation of the Federal States with the Federation and between the States, each Federal State shall maintain an agency responsible for matters relating to the protection of the constitution.

Section 3. Tasks of the Protection of the Constitution Agencies

(1) The protection of the constitution agencies of the Federation and the Federal States shall be tasked with the collection and analysis of information, especially of such information, intelligence and documents relating to individuals or subject-matters, concerning

1. efforts directed against the free democratic basic order, the existence or the security of the Federation or one of its States or aimed at unlawfully hampering constitutional bodies of the Federation or one of its States or their members in the performance of their duties;

2. activities threatening security or intelligence activities carried out on behalf of a foreign power within the area where this Act applies;

3. efforts within the area where this Act applies, which jeopardise foreign concerns of the Federal Republic of Germany by the use of violence or preparation thereof;

4. efforts within the area where this Act applies, directed against the idea of international understanding (Art. 9, par. 2 of the Basic Law refers), especially against the peaceful coexistence of peoples (Art. 26, par. 1 of the Basic Law refers).

(2) The protection of the constitution agencies of the Federation and the

5 The German constitution.
Federal States shall contribute
1. to screening individuals who are to be entrusted with facts, materials or intelligence which must be kept secret in the public interest, or who are to have or can gain access to such information;
2. to screening individuals who are employed or are to be employed in sensitive areas of facilities of a vital or defence-related interest;
3. to technical security measures to prevent unauthorised persons from gaining access to facts, materials or intelligence which must be kept secret in the public interest.


(3) The protection of the constitution agencies shall be subject to the general rules of law (Art. 20 of the Basic Law refers).

Section 4. Definition of Terms
(1) Within the meaning of this Act,
   a) any politically motivated, target-oriented and purposeful behaviour within or for an association of individuals which aims at disrupting the independence of the Federation or one of its States from foreign rule, their national unity or territorial integrity shall be considered an effort directed against the existence of the Federation or one of its States;
   b) any politically motivated, target-oriented and purposeful behaviour within or for an association of individuals which aims at seriously prejudicing the functioning of the Federation, any of its States or their organs shall be considered an effort directed against the security of the Federation or one of its States;
   c) any politically motivated, target-oriented and purposeful behaviour within or for an association of individuals which aims at removing any of the constitutional principles mentioned in subsection 2 below or rendering them ineffective shall be considered an effort directed against the free democratic basic order.

Anybody who firmly supports the efforts and objectives of an associa-
tion of individuals shall be considered acting for it. The collection and analysis of information under section 3, subsection 1 above shall not be permissible unless there is hard evidence of such efforts as defined by this Act. Any behaviour of individuals who are not acting in or for an association of individuals shall be considered an effort as defined by this Act if such behaviour is aimed at using violence or due to its implications is capable of severely damaging any of the interests protected by this Act.

(2) The free democratic basic order as defined by this Act embodies:

a) the right of the people to exercise the state authority it has been vested with by means of elections and votes and through specific legislative, executive and judicial organs and to elect the body representing the people in general, direct, free, fair and secret elections;

b) the commitment of the legislature to the constitutional order and the commitment of the executive and judiciary to law and justice;

c) the right to form and exercise a parliamentary opposition;

d) the replaceability of the government and its accountability to parliament;

e) the independence of the courts;

f) the exclusion of any despotic and arbitrary rule; and

g) the human rights as laid down in the Basic Law.

Section 5. Delimitations of the Responsibilities of the Protection of the Constitution Agencies

(1) The state offices for the protection of the constitution shall collect information, particulars, intelligence and data to fulfil their tasks, analyse them and pass them to the Federal Office for the Protection of the Constitution and to the state offices for the protection of the constitution as far as they need them for the proper performance of their tasks.

(2) The Federal Office for the Protection of the Constitution may collect information, particulars, intelligence and data as defined by section 3 in a Federal State in consultation with the state office for the protection of the constitution concerned if efforts and activities as defined by section 3, subsection 1, nos. 1-4

1. are directed in whole or in part against the Federation;
2. extend beyond the borders of a Federal State;
3. affect foreign concerns of the Federal Republic of Germany; or
4. if a state office for the protection of the constitution requests the involvement of the Federal Office.

For a number of similar cases, summary consultation is possible.

(3) The Federal Office for the Protection of the Constitution shall inform the state offices for the protection of the constitution of all data which the states need to know for the purpose of protecting the constitution.

Section 6. The Sharing of Information between the Protection of the Constitution Agencies

In order to fulfil their duties under section 5 (obligation to share information), the protection of the constitution agencies are obliged to maintain joint files at the Federal Office for the Protection of the Constitution, which they use by means of an automated system. These files shall only contain such information which is necessary to find relevant records and to identify individuals, which as such is a prerequisite for finding those records. The storage of personal data shall not be allowed unless the conditions laid down under sections 10 and 11 do exist. Other agencies shall not be authorised to use the automated system to request information. In its function as a data storing body, an office for the protection of the constitution shall be responsible in terms of the general provisions regarding data protection only for those data which it has entered itself; it shall be the only body which is authorised to modify, block or erase such data. The data storing body must be identifiable. The Federal Office for the Protection of the Constitution shall take the technical and organisational measures under section 9 of the Federal Data Protection Act for the joint files. Text files or files which contain more information than that specified in sentence 2 above shall not be maintained under the conditions laid down in this section except for very limited areas of application for the purpose of investigating activities threatening security or intelligence activities carried out on behalf of a foreign power or efforts aimed at using violence or preparing for the use of violence. The right of access shall be restricted to individuals who are directly entrusted with working in such an area of application; the necessity of entering
supplementary texts into the file shall be substantiated in the directive on file management (section 14).

Section 7. The Federation’s Authority to issue Directives
In case of an offence against the constitutional order of the Federation, the Federal Government shall be authorised to give the state executive agencies directives essential to the cooperation between the Federal States and the Federation in matters relating to the protection of the constitution.

PART II Federal Office for the Protection of the Constitution

Section 8. Powers of the Federal Office for the Protection of the Constitution

(1) The Federal Office for the Protection of the Constitution may collect, process and use information including personal data needed to fulfil its tasks in so far as this does not conflict with the applicable provisions of the Federal Data Protection Act or specific regulations therein. A request for the transfer of personal data made by the Federal Office for the Protection of the Constitution shall only include those personal data needed to provide information. The legitimate interests of the data subject shall only be prejudiced to an unavoidable extent.

(2) The Federal Office for the Protection of the Constitution may use methods, materials and instruments such as trusted persons and informants, surveillance, image and sound recordings, cover documents and cover licence plates for the clandestine collection of information which are to be specified in a service regulation at the same time regulating the responsibility for ordering such collection of information. The service regulation is subject to the consent of the Federal Ministry of the Interior, who notifies the Parliamentary Control Panel.

(3) Police powers or authorities to give directives shall not be within the scope of the competences of the Federal Office for the Protection of the Constitution; it may not request the police to take action which it is not authorised to take itself.

(4) If personal data are collected from the data subject with his consent, the purpose of collection shall be specified. The data subject shall be
advised of the fact that his giving the required information is a voluntary act.

(5) From among several appropriate measures, the Federal Office for the Protection of the Constitution shall select the one prospectively least restrictive for the data subject. A measure shall not cause a prejudice being recognisably disproportionate to the intended result.

Section 8a. Special requests for information

(1) In individual cases, the Federal Office for the Protection of the Constitution may request information from providers of commercial postal or teleservices regarding data which have been stored in connection with the establishment, terms and conditions, amendments to or termination of a contract for postal services or teleservices (inventory data), where this is necessary for the Federal Office in discharging its tasks.

(2) In individual cases, the Federal Office for the Protection of the Constitution may request information from

1. airlines, regarding the names and addresses of customers, transport services used and attendant details, in particular with respect to check-in and departure and the booking process,
2. banks, financial services institutions and financial enterprises, regarding accounts, account holders and other parties authorised to access accounts, other parties involved in transactions and information on cash movements and deposits, in particular with respect to account balances and payments into and out of accounts,
3. providers of commercial postal services or parties involved in the provision of such services, regarding details of postal traffic,
4. providers of commercial telecommunications services or parties involved in the provision of such services, regarding traffic data pursuant to Section 96 (1), nos. 1 to 4 of the Telecommunications Act and other traffic data required in establishing and maintaining telecommunications and
5. providers of commercial teleservices and parties involved in the provision of such services, regarding
   a) characteristics to identify the user of a teleservice,
   b) information on the beginning and end and the scope of such use
and
c) information on the teleservices employed by the user, where this is necessary in pursuing investigations into efforts or activities and where there are actual indications of serious threats to the interests stated in Section 3 (1). In the case of Section 3 (1), no. 1, this shall apply solely to efforts which, by intention or by their fundamental nature, are conducive
1. to inciting hatred or arbitrary measures against parts of the population or to attacking their human dignity through insults, malicious disparagement or slander, thereby promoting a willingness to use violence and to disrupt social harmony or
2. to the use of violence or preparations for violence, including advocating, causing or supporting the use of violence, also by supporting organisations which instigate, advocate or threaten attacks on persons or property.

(3) Orders pursuant to subsection 2 may only be directed against persons who
1. are suspected on the basis of actual indications of specifically promoting serious threats as defined in subsection 2, or
2. are suspected on the basis of certain facts
   a) of employing the service concerned for a person pursuant to number 1. with regard to information pursuant to subsection 2, sentence 1, nos. 1, 2 and 5, or
   b) of receiving or passing on messages originating from or intended for a person pursuant to number 1 with regard to information pursuant to subsection 2, sentence 1, nos. 3 and 4 or, in the case of subsection 2, sentence 1, no. 4, of arranging for a person pursuant to number 1 to use their connection.

(4) The competence for orders pursuant to subsection 2, sentence 1, no. 1 shall be stipulated in a service regulation which shall require the consent of the Federal Ministry of the Interior. Orders pursuant to subsection 2, sentence 1, nos. 2 to 5 shall be applied for in writing by the head of the agency or his deputy, stating the attendant grounds. In the case of information pursuant to number 2 the application may also be filed by a member of staff of the Federal Office for the Protection of the Constitution who is qualified to hold judicial office. The federal
ministry authorised by the Federal Chancellery shall be responsible for orders pursuant to subsection 2, sentence 1, nos. 2 to 5. Orders for the disclosure of information on data arising in the future shall be limited to a maximum period of three months. Extensions of such orders for subsequent periods of no more than three months in each instance shall be admissible upon application, provided that the conditions pertaining to the order continue to apply. The Federal Office for the Protection of the Constitution shall inform the data subject of orders pursuant to subsection 2, sentence 1, nos. 1 and 2 as soon as it can be ruled out that the purpose of the measure might be jeopardised.

(5) The competent federal ministry pursuant to subsection 4, sentence 4, shall notify the G10 Commission (Section 1 (2) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications) of orders pursuant to subsection 2, sentence 1, nos. 3 to 5 on a monthly basis, prior to their enforcement. In cases of imminent danger, the competent federal ministry may also order the enforcement of decisions prior to notifying the Commission. The G10 Commission shall examine ex-officio or on the basis of complaints whether requests for information are admissible and necessary. Section 15 (2) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall be applied subject to the proviso that the Commission’s supervisory powers extend to the entire scope of collection, processing and use of the personal data obtained pursuant to subsection 2, nos. 3 to 5. The competent federal ministry is to revoke forthwith any decisions on information which the G10 Commission declares inadmissible or unnecessary. In this case, an absolute ban on use of the data concerned shall apply and the data shall be erased forthwith. Section 4 of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall be applied mutatis mutandis to the processing of data collected pursuant to subsection 2, sentence 1, nos. 3 to 5. Section 12 (1) and (3) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall apply mutatis mutandis.

(6) The competent federal ministry pursuant to subsection 4, sentence 4 shall notify the Parliamentary Control Panel of orders pursuant to subsection 2 at intervals of no more than six months, in particular provid-
ing an overview of the grounds for the measures carried out in the reporting period concerned, the scope and duration of such measures, the results and the attendant costs. The Control Panel shall furnish the German Bundestag with an annual report on implementation of the measures and on the nature and scope of such measures and the grounds for their implementation, observing the principles stipulated in Section 10 (1) of the Parliamentary Control Panel Act.

(7) Orders shall be submitted in writing to the party obliged to furnish information to the extent to which this is necessary in order to enable said party to fulfil its obligation. The party obliged to furnish information must not notify data subjects or third parties of orders and transferred data.

(8) The powers pursuant to subsection 2, sentence 1, nos. 3 to 5 shall only apply to the Protection of the Constitution Agencies of the Federal States on condition that the relevant state legislation sets out provisions equivalent to those stipulated in subsection 5 regarding the procedure, the involvement of the G10 Commission, processing of the collected data and notification of the data subject, parliamentary control equivalent to that stipulated in subsection 6 and an obligation to report to the Parliamentary Control Panel of the Federation on measures carried out, duly applying subsection 6, sentence 1, second clause for the reports pursuant to subsection 6, sentence 2. The obligations to provide for equivalent parliamentary control pursuant to subsection 6 shall also apply to the powers pursuant to subsection 2, nos. 1 and 2.

(9) The fundamental right of the privacy of correspondence, posts and telecommunications (Article 10 of the Basic Law) shall be curtailed in accordance with subsection 2, sentence 1, nos. 3 to 5 and subsections 5 to 8.

Section 9. Specific Forms of Data Collection

(1) The Federal Office for the Protection of the Constitution may collect information, particularly personal data, with the means defined in section 8, subsection 2 if facts give reason to believe that

1. in this way intelligence on efforts or activities referred to in section 3, subsection 1 can be gained or sources won, who are necessary to
investigate such intelligence, or
2. this is necessary to protect the staff, facilities, objects and sources
   of the Federal Office for the Protection of the Constitution against
   activities posing a threat to security or against activities by hostile
   secret services.

The collection of information pursuant to sentence 1 shall not be per-
missible if the investigation of the facts and circumstances is possible
in a way less restrictive for the data subject. As a rule, restrictions can
be considered smaller if the information is to be gained from generally
accessible sources or by an inquiry as defined in section 18, subsec-
tion 3. Employing assets according to section 8, subsection 2 must not
be recognisably disproportionate to the importance of the matter to be
investigated. The measure shall be stopped as soon as its purpose has
been achieved or if there are indications that it cannot be achieved at
all or by employing these assets.

(2) Technical means of eavesdropping on or clandestinely recording pri-
ivate conversations in dwelling places shall only be employed if it is
necessary, in particular cases, to ward off imminent general dangers or
imminent dangers to individual persons’ lives and if the police cannot
adequately protect the legal interests exposed in time. Sentence 1 ap-
plies mutatis mutandis for covertly implementing technical means of
taking pictures and making video recordings. The implementation of
measures under sentence 1 and 2 shall be ordered by the head of the
Federal Office for the Protection of the Constitution or his deputy if a
judicial decision cannot be obtained in time. Such a decision shall
then be sought without delay from the local court of the district where
the Federal Office for the Protection of the Constitution has its seat.
The procedure shall be governed by the provisions of the law on pro-
cedure in family matters and matters of non-contentious jurisdiction.
The data collected shall only be used in accordance with section 4,
subsection 4 of the Act Restricting the Privacy of Correspondence,
Posts and Telecommunications. Besides, technical means as defined
by sentence 1 and 2 shall be implemented to protect individuals while
they are operating in dwelling places, in so far as it is necessary to
ward off dangers to their lives, health or freedom. The implementation
of measures under sentence 8 shall be ordered by the head of the Fed-
eral Office for the Protection of the Constitution or his deputy. Besides for the purpose under sentence 8, the Federal Office for the Protection of the Constitution shall only use the data thus collected to prevent threats in the course of the fulfilment of its tasks as defined by section 3, subsection 1, nos. 2 - 4 and to communicate data under section 4, subsection 4, nos. 1 - 2 of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications. Their use shall only be admissible if the lawfulness of the measure has been declared by a judge beforehand; in case of imminent danger, the judicial decision shall be sought subsequently without delay. Section 4, subsection 6 of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall apply mutatis mutandis. The fundamental right of the inviolability of the home (Art. 13 of the Basic Law refers) shall be restricted accordingly.

(3) Where the collection of data in accordance with subsections 2 and 1 is concerned, the nature and importance of which is tantamount to a restriction of letter, postal and telecommunications privacy, in particular comprising eavesdropping on and recording of private conversations with clandestine technical means,
1. the data subject shall be informed of the measure after its termination, as soon as it can be ruled out that the purpose of the measure is jeopardised, and
2. the Parliamentary Control Panel shall be notified.

(4) In order to fulfil its tasks as defined by section 3, subsection 1, nos. 2 – 4, the Federal Office for the Protection of the Constitution, under the provisions of section 3, subsection 1 of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications, may use technical means for the purpose of identifying the position of an activated cell phone terminal and serial numbers and card codes. The measure shall only be admissible if the purpose of the surveillance action could not be attained at all or would be rendered much more difficult without this identification being effected. Section 4 of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall apply accordingly to the processing of the data. Personal data of a third party shall only be collected in the course of such measures if this is unavoidable on technical grounds to attain the purpose as defined in
sentence 1. The use of these data shall be strictly prohibited, and the data shall be erased immediately after the measure has been terminated. Section 8, subsections 9 and 10 shall apply mutatis mutandis. The fundamental right of letter, postal and telecommunications privacy (Art. 10 of the Basic Law refers) is restricted accordingly.

**Section 10. Storage, Modification and Use of Personal Data**

(1) To fulfil its tasks, the Federal Office for the Protection of the Constitution may store, modify and use personal data if

1. there are actual indications of efforts or activities pursuant to section 3, subsection 1,
2. this is necessary to the investigation and analysis of efforts or activities pursuant to section 3, subsection 1 or
3. the Federal Office for the Protection of the Constitution takes action under section 3, subsection 2.

(2) (Is repealed.)

(3) The Federal Office for the Protection of the Constitution shall restrict the duration of storage to the extent necessary to fulfil its tasks.

**Section 11. Storage, Modification and Use of Personal Data on Minors**

(1) Pursuant to Section 10, the Federal Office for the Protection of the Constitution may only store, modify and use data on minors under 16 years of age in the personal records kept on them if there are actual indications of the minor planning, committing or having committed a criminal offence as defined in Section 3 (1) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications. The storage of data or information on the behaviour of minors under 16 years of age in files shall not be permissible. Sentence 2 shall not apply to minors over 14 years of age where, on the basis of circumstances pertaining to the individual case concerned, it cannot be ruled out that the storage of data may be necessary in order to avert a serious threat to a person’s life or limb.

(2) After two years, the necessity of the storage of data on minors in files or personal records kept on them shall be reviewed, and after five years at the latest they shall be erased, provided that no further intelligence under section 3, subsection 1 has been obtained after the data
Section 12. Correction, Erasure and Blocking of Personal Data in Files

(1) Incorrect personal data stored in files shall be corrected by the Federal Office for the Protection of the Constitution.

(2) Personal data stored in files shall be erased by the Federal Office for the Protection of the Constitution if their storage was inadmissible or knowledge of them is no longer required for the fulfilment of its tasks. The data shall not be erased if there is reason to believe that erasure would impair legitimate interests of the data subject. In this case the data shall be blocked and shall only be transferred with the data subject’s consent.

(3) When dealing with particular cases, the Federal Office for the Protection of the Constitution shall check within given periods, after five years at the latest, if stored personal data must be corrected or erased. Personal data stored on efforts as defined in section 3, subsection 1, no. 1 shall be erased not later than ten years and on efforts as defined in section 3, subsection 1, nos. 3 - 4 not later than fifteen years following the date of storage of the last relevant information, unless the head of the agency or his deputy by way of exception decides differently in an individual case.

(4) Personal data stored exclusively for the purpose of data protection control or data security or to ensure proper operation of a data processing system may only be used for such purposes.

Section 13. Correction and Blocking of Personal Data in Records

(1) If it is ascertained by the Federal Office for the Protection of the Constitution that personal data stored in records are incorrect or if their correctness is contested by the data subject, a note to this effect shall be made in the record or it shall be recorded by some other means.

(2) Personal data shall be blocked if it is ascertained by the Federal Office for the Protection of the Constitution in particular cases that without blocking, legitimate interests of the data subject would be impaired and the data are no longer required for the future fulfilment of its tasks. Blocked data shall be marked accordingly; they may no longer be used or transferred. The blocking of data can be repealed if the
Section 14. Directives on File Management

(1) For any automated file maintained at the Federal Office for the Protection of the Constitution under sections 6 and 10 a directive on file management which is subject to the approval of the Federal Ministry of the Interior, shall specify:
1. the file name,
2. the purpose of the file,
3. the conditions to be complied with when storing, transferring and using the data (group of individuals concerned, categories of the data),
4. supply or input,
5. access authorisation,
6. time periods for reviews, duration of storage,
7. recording of access.

The Federal Commissioner for Data Protection and Freedom of Information shall be heard prior to issuing a directive on file management.

(2) The storage of personal data shall be restricted to the extent necessary. The necessity of further maintaining or amending the files shall be checked at reasonable intervals.

(3) As regards automated personal text files, the directive on file management shall restrict access to individuals who are directly involved in activities in the field which the text file is attributed to; extracts from text files may not be transferred without the pertinent explanatory documents.

Section 15. Provision of Information to the Data subject

(1) The Federal Office for the Protection of the Constitution shall provide the data subject, at his/her request, with information free of charge on personal data stored on him/her, if he/she refers to concrete matters and proves to have a special interest in the information which he/she has asked for.

(2) The information shall not be provided if
1. this would prejudice the proper fulfilment of tasks,
2. this could expose sources or if it is to be feared that the Federal Office for the Protection of the Constitution's knowledge or its
modus operandi might be explored,
3. this would impair public safety or otherwise be detrimental to the Federation or a Federal State, or if
4. the data or the fact that they are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party.

The decision shall be made by the head of the Federal Office for the Protection of the Constitution or by a staff member explicitly authorised by him.

(3) The obligation to provide information shall not include information on the origin of the data and the recipients of the data transferred.

(4) Reasons for the refusal to provide information need not be given if this jeopardised the purpose being pursued by refusing to provide the information. The reasons for the refusal shall be taken on record. In case of a refusal to provide information the data subject shall be informed of the legal basis for a reason not being given and of the fact that he/she may appeal to the Federal Commissioner for Data Protection, who shall, at his request, be supplied with the information unless the Federal Ministry of the Interior determines in a particular case that this would jeopardise the security of the Federation or a Federal State. Information given to the data subject by the Federal Commissioner shall not permit any conclusions to be drawn as to the state of information held by the Federal Office for the Protection of the Constitution unless the latter agrees to more extensive information being provided.

Section 16. Accountability of the Federal Office for the Protection of the Constitution

(1) The Federal Office for the Protection of the Constitution shall notify the Federal Ministry of the Interior of its activities.

(2) This notification pursuant to subsection 1 at the same time serves the information of the public by the Federal Ministry of the Interior on efforts and activities as defined in section 3, subsection 1 and is effected at least once a year in a comprehensive report. In this connection, personal data may be disclosed, too, if the understanding of contextual
circumstances or the presentation of organisations or unorganised groupings necessitate disclosure and if the public's interest prevails on the interest of the data subject. The federal budget's subsidies to the Federal Office for the Protection of the Constitution and the Military Counterintelligence Service and the respective total number of staff members shall be published in the annual report.

Part III Provisions for the Transfer of Data

Section 17. Admissibility of Requests

(1) If the transfer of personal data is requested under the provisions of this part, only those data shall be transferred which are known to the authority requested or which can be taken from generally accessible sources.

(2) Subsection 1 shall not apply to particular requests made by the offices for the protection of the constitution, the Military Counterintelligence Service and the Federal Intelligence Service for such data learnt in the course of the performance of border police duties. The admissibility of such particular requests and their execution shall be regulated in service instructions by the Federal Ministry of the Interior in consultation with the Federal Chancellery and the Federal Ministry of Defence. The Federal Ministry of the Interior shall notify the Parliamentary Control Panel of their issue and of necessary amendments. Sentences 2 and 3 shall not apply to particular requests between authorities of the same Federal State.

(3) Where necessary for the purpose of discharging the tasks of the Federal Office for the Protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service, these agencies may enter an alert in the police information system, requesting notification when a person or an object specified in Article 36(1) of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) is found, provided that the conditions of Article 36(3) of Council Decision 2007/533/JHA are met and there are actual indications of cross-border movement. Upon such persons or objects being found, the body from which information is requested may transfer information to the alerting authority pursuant to Article 37 of Council
Decision 2007/533/JHA. Such alerts shall be ordered by the head of the agency, his or her deputy or a specially commissioned member of staff who is qualified to hold judicial office. The alert shall be limited to a period of no more than six months and may be ordered repeatedly. Upon the conditions pertaining to the alert ceasing to apply, the purpose of the measure being achieved or upon it becoming apparent that the purpose cannot be achieved, the alert shall be erased forthwith. Section 8a (6) shall apply mutatis mutandis subject to the proviso that, in place of the competent federal ministry pursuant to Section 8a (4), sentence 4, the Federal Ministry of Defence shall be competent for alerts by the Military Counterintelligence Service and the Federal Chancellery shall be competent for alerts by the Federal Intelligence Service.

Section 18. Transfer of Information to the Offices for the Protection of the Constitution

(1) The authorities of the Federation, of the federal institutions of public law, the public prosecutors’ offices and, subject to the public prosecutors’ authority to give instructions as regards subject matters, the police authorities, the authorities of the customs investigation service and other customs offices performing tasks under the Act on the Federal Police, on their own initiative, shall notify the Federal Office for the Protection of the Constitution or the state offices for the protection of the constitution of the information, including personal data, having come to their knowledge, indicative of activities threatening security or intelligence activities carried out on behalf of a foreign power or efforts within the area where this Act applies which by use of violence or preparation thereof are directed against the interests protected by this Act as defined in section 3, subsection 1, nos. 1, 3 and 4. Obligations to transfer information under the Military Counterintelligence Service Act or the Federal Intelligence Service Act beyond those defined in sentence 1 shall not be affected. Sentence 1 shall not apply to the transfer of information between authorities of the same Federal State.

(1a) The Federal Office for Migration and Refugees shall notify the Federal Office for the Protection of the Constitution and the foreigners authorities of a Federal State shall notify the state Protection of the Constitu-
tion Agency, on their own initiative, of information, including personal data, having come to their knowledge, on efforts or activities as defined in section 3, subsection 1 if there are actual grounds to believe that the transfer of such information is required for them to fulfil the tasks of the offices for the protection of the constitution. Transfer of these personal data to foreign public authorities and supranational and interstate authorities pursuant to Section 19 (3) shall also be prohibited where precluded by overriding legitimate interests of third parties. The Federal Office for Migration and Refugees shall be consulted prior to effecting transfer pursuant to Section 19 (3). Section 8a (6) shall apply mutatis mutandis to such transfers by the Federal Office for the Protection of the Constitution.

(2) The public prosecutors' offices and, subject to the public prosecutors' authority to give instructions as regards subject matters, the police authorities, the authorities of the customs investigation service and other customs offices performing tasks under the Act on the Federal Police, and the Federal Intelligence Service, on their own initiative, may also notify the Federal Office for the Protection of the Constitution or the state offices for the protection of the constitution of any other information, including personal data, having come to their knowledge on efforts as defined in section 3, subsection 1 if there are actual grounds to believe that such a transfer of information is required for them to fulfil the tasks of the offices for the protection of the constitution. Subsection 1, sentence 3 shall apply.

(3) The Federal Office for the Protection of the Constitution may request the public prosecutors' offices and, subject to the public prosecutors' authority to give instructions as regards subject matters, the police authorities and other agencies to transfer information, including personal data, required for it to fulfil its tasks, if they cannot be gained from generally accessible sources or only by means of disproportionate efforts or in a way more impairing for the data subject. Under the same conditions, the state offices for the protection of the constitution may request such information from

1. authorities of the Federation and the federal institutions of public law,
2. public prosecutors' offices and, subject to the public prosecutors'
authority to give instructions as regards subject matters, police authorities of the Federation and the Federal States.

(3a) In discharging their duties, the Federal Office for the Protection of the Constitution and the authorities of the Federal States for the protection of the constitution may request the fiscal authorities to provide information as to whether a corporation, association or estate meets the conditions of Section 5 (1), no. 9 of the Corporation Tax Act. The fiscal authorities shall furnish the information to the requesting authorities pursuant to sentence 1.

(4) If the transfer of information pursuant to subsection 3, sentence 1 jeopardised the purpose of the measure or impaired the data subject in a disproportionate manner, the Federal Office for the Protection of the Constitution, when fulfilling its tasks specified in section 3, subsection 1 nos. 2 - 4 and monitoring terrorist efforts, may consult official registers.

(5) Requests pursuant to subsection 3 shall be taken on record. The consultation under subsection 4 shall be recorded by the Federal Office for the Protection of the Constitution, detailing the purpose and the grounds of the measure, the authority requested and the source file; the records shall be kept separately, protected from unauthorised access and destroyed at the end of the calendar year following the year of their issue.

(6) The transfer of personal data learnt by way of a measure pursuant to section 100a of the Code of Criminal Procedure shall only be admissible under the provisions of subsections 1, 2 and 3 if there are actual grounds to believe that an individual is planning, committing or has committed one of the criminal offences defined in Section 3 (1) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications. Section 4, (1) and (4) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications shall apply mutatis mutandis to information and documents transferred to an office for the protection of the constitution under sentence 1.

Section 19. Transfer of Personal Data by the Federal Office for the Protection of the Constitution

(1) The Federal Office for the Protection of the Constitution may transfer
personal data to national public authorities if this is required for it to fulfil its tasks or if the data are needed by the recipient for the purpose of protecting the free democratic basic order or for any other purpose of public security. The recipient may only use the data transferred for the purpose they were transferred for unless otherwise provided by law.

(2) The Federal Office for the Protection of the Constitution may transfer personal data to authorities of the stationed forces, in so far as the Federal Republic of Germany is obliged to do so pursuant to section 3 of the Agreement to Supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to Foreign Forces Stationed in the Federal Republic of Germany of 3 August 1959 (Federal Law Gazette 1961 II, p. 1183, 1218).

(3) The Federal Office for the Protection of the Constitution may transfer personal data to foreign public authorities and supranational and interstate authorities if such a transfer is required for it to fulfil its tasks or to safeguard substantial security interests of the recipient. Data shall not be transferred if their transfer conflicts with foreign concerns of the Federal Republic of Germany or with overriding legitimate interests of the data subject. The transfer shall be taken on record. The recipient’s attention shall be drawn to the fact that the data transferred may only be used for the purpose they were transferred to him and that the Federal Office for the Protection of the Constitution reserves the right to inquire about the use of the data.

(4) Personal data may only be transferred to other authorities if this is required to protect the free democratic basic order or the existence or security of the Federation or one of its States or to ensure security of vital or defence-related installations as defined in section 1, subsection 4 of the Security Vetting Act. The transfer of data under sentence 1 is subject to prior consent of the Federal Minister of the Interior. The Federal Office for the Protection of the Constitution shall keep records of the purpose and the grounds, the source file and the recipient of the data transferred under sentence 1. The records shall be kept separately, protected from unauthorised access and destroyed at the end of the calendar year following the year of their issue. The recipient may only use the data transferred for the purpose they were transferred to
him. His attention shall be drawn to the fact that use of the data is re-
stricted and that the Federal Office for the Protection of the Constitu-
tion reserves the right to inquire about the use of the data. The Federal
Office for the Protection of the Constitution shall notify the data sub-
ject of the transfer of the personal data as soon as the proper fulfilment
of its tasks is no longer jeopardised. Sentences 2 and 3 shall not apply
if personal data are transferred for the purpose of collecting data pur-
suant to section 8, subsection 1, sentence 2.

(5) Subsection 4 shall not apply when personal data are transferred for
the purpose of collecting data pursuant to Section 8 (1), sentence 2.

Section 20. Transfer of Information by the Federal Office for the
Protection of the Constitution to Law Enforcement and Security
Agencies in Matters relating to State Security and the Protection of
the Constitution

(1) The Federal Office for the Protection of the Constitution, on its own
initiative, shall provide the public prosecutors‘ offices and, subject to
the public prosecutors‘ authority to give instructions as regards sub-
ject matters, the police authorities with information, including per-
sonal data, having come to its knowledge if there are actual grounds to
believe that such a transfer of information is required to prevent or
prosecute crimes against the state. Crimes pursuant to sentence 1 are
criminal offences as defined in sections 74a and 120 of the Judicature
Act and other criminal offences which because of their objective, the
perpetrator's motive or his association with an organisation provide
actual grounds to believe that they are directed against the interests to
be protected under Art. 73, par. 10, sub-par. b or c of the Basic Law.
The Federal Office for the Protection of the Constitution, on its own
initiative, shall provide the Federal Intelligence Service with informa-
tion, including personal data, having come to its knowledge, if there
are actual grounds to believe that such a transfer of information is re-
quired by the recipient to perform its legal task.

(2) The police authorities may request the Federal Office for the Protec-
tion of the Constitution to transfer the information, including personal
data, needed to prevent crimes against the state. The Federal Intelli-
gence Service may request the Federal Office for the Protection of the
Constitution to transfer information, including personal data, required to perform its tasks.

**Section 21. Transfer of Information by the State Offices for the Protection of the Constitution to Law Enforcement and Security Agencies in Matters relating to State Security and the Protection of the Constitution**

(1) The state offices for the protection of the constitution shall provide the public prosecutors‘ offices and, subject to the public prosecutors‘ authority to give instructions as regards subject matters, the police authorities with information, including personal data, under the provisions of section 20, subsection 1, sentences 1 and 2 and subsection 2, sentence 1. Sentence 1 shall not apply to the transfer of information between the authorities of the same Federal State.

(2) The state offices for the protection of the constitution shall provide the Federal Intelligence Service and the Military Counterintelligence Service with information, including personal data, under the provisions of section 20, subsection 1, sentence 3 and subsection 2, sentence 2.

**Section 22. Transfer of Information by the Public Prosecutors‘ Offices and the Police Authorities to the Military Counterintelligence Service**

For the transfer of information, including personal data, by the public prosecutors‘ offices and, subject to the public prosecutors‘ authority to give instructions as regards subject matters, the police authorities, the authorities of the customs investigation service and other customs offices performing tasks under the Act on the Federal Police, to the Military Counterintelligence service, section 18 shall apply mutatis mutandis.

**Section 22a. Project-related joint files**

(1) The Federal Office for the Protection of the Constitution may set up a joint file for the duration of temporary project-related cooperation with the Protection of the Constitution Agencies of the Federal States, the Military Counterintelligence Service, the Federal Intelligence Service, the police authorities at Federation and Federal State level and the Central Office of the German Customs Investigation Service. In ac-
cordance with the remits and powers of the authorities stated in sentence 1, such project-related cooperation shall be aimed at exchanging and jointly evaluating information with regard to efforts which are directed against the interests stated in Section 3 (1), nos. 1 to 4 through the use of violence or preparatory actions for violence. Personal data pertaining to efforts pursuant to sentence 2 may be used via recourse to the joint file by the authorities involved in the project-related cooperation within the scope of their powers where necessary in connection with discharging their tasks. The further use of such personal data shall be subject to the provisions on the use of data such as apply specifically to the respective authorities involved.

(2) The entry of personal data in the joint file shall be subject to the provisions on communication such as apply to the respective cooperating authorities, with the proviso that entry shall be permissible only when communication of the data to all authorities involved in the project-related cooperation is permissible. Entry shall further only be permissible when the authority entering the data is also permitted to store the data in files of its own. The authority entering the data is to identify the data.

(3) Section 6, sentence 5 to 7 and Section 14 (2) shall apply mutatis mutandis to the keeping of a project-related joint file. Section 15 shall be applied subject to the proviso that the Federal Agency for the Protection of the Constitution shall issue the information in consultation with the authority bearing responsibility for data protection pursuant to sentence 1 and the participating authority concerned shall verify the admissibility of issuing the information according to the provisions to which it is subject.

(4) The joint file pursuant to sentence 1 shall be limited in duration to a maximum of two years. The aforesaid period may be extended twice by a further period of one year in each instance, if the objective of the project-related cooperation has not yet been attained at the end of the project and the file remains necessary for the purpose of attaining the objective.

(5) The correction, blocking and erasure of data on a person by the authority which has entered the data shall be subject mutatis mutandis to the provisions on correction, blocking and erasure of the data
which are applicable to the authority concerned.

(6) For the joint file, the Federal Office for the Protection of the Constitution shall stipulate the information pursuant to Section 14 (1), sentence 1, nos. 1 to 7 in a directive on file management, together with the following additional details and stipulations:

1. the legal basis for the file,
2. the type of personal data to be stored,
3. the type of personal data serving to render the file accessible,
4. conditions, subject to which data stored in the file may be transferred, further stipulating to whom such data may be communicated and according to which procedures,
5. in consultation with the authorities participating in the project-related cooperation, the latters' organisational units which are authorised to enter and retrieve data,
6. immediate notification by the authorities sharing the joint file of the authority entering data in the case of indications that the entered data is incorrect, examination and, where necessary, prompt modification, correction or erasure of such data by the authorities which entered them,
7. the possibility of entering additional data to the data already stored on a person by the authorities sharing the joint file,
8. documentation of the time of retrieval, the necessary information to identify the retrieved data record and the authority responsible for retrieval, for each case of data retrieval from the joint file by the Federal Office for the Protection of the Constitution for the purposes of monitoring data protection, including specification of the purpose for which the documented data are to be used and their erasure deadline and
9. the responsibility of the Federal Office for the Protection of the Constitution for claims for compensation asserted by the data subject pursuant to Section 8 of the Federal Data Protection Act.

The directive on file management shall require the approval of the Federal Ministry of the Interior and the supreme Federal or Land authorities responsible for supervision of the authorities involved. The Federal Commissioner for Data Protection and Freedom of Information shall be consulted prior to issuing a directive on file management.
Section 14 (3), clause 1 shall apply mutatis mutandis.

**Section 23. Prohibition of Transfer**
The transfer of information pursuant to the regulations of this part shall be prohibited if
1. the transferring authority can determine that considering the character of the information and the manner of their collection the legitimate interests of the data subject prevail on the public interest in the transfer of such information,
2. substantial security interests necessitate the withholding of information, or if
3. it is contrary to particular legal provisions for the transfer of data; the obligation to maintain legal, professional or official secrecy not being based on legal provisions shall not be affected.

**Section 24. Protection of Minors**
(1) Under the provisions of this Act, information, including personal data, on the behaviour of minors may be transferred, if the requirements for storage as defined in Section 11 (1), sentence 1 are met. If they are no longer met, the transfer of such information shall only remain admissible if it is of considerable importance to ward off a great danger or to prosecute a criminal offence.

(2) Under the provisions of this Act, information, including personal data, on the behaviour of minors under 16 years of age may not be transferred to foreign public authorities or supranational or interstate authorities. By way of derogation from the aforesaid provision, information, including personal data, on the behaviour of minors over 14 years of age may be transferred where, on the basis of circumstances pertaining to the individual case concerned, it cannot be ruled out that such transfer may be necessary in order to avert a serious threat to a person’s life or limb or where there are actual indications that transfer is necessary in order to prosecute a criminal offence specified in Section 3 (1) of the Act Restricting the Privacy of Correspondence, Posts and Telecommunications.

**Section 25. Obligations of the Recipient**
The recipient shall check if the personal data transferred under the
provisions of this Act are needed to perform his duties. If the check results in the data not being needed, he shall destroy the records. Destruction may not be necessary if separation from other information needed to perform the tasks is not possible at all or only with disproportionate efforts; in this case the data shall be blocked.

Section 26. Obligation to transfer additional Information
If personal data, following their transfer pursuant to the provisions of this Act, turn out to be incomplete or incorrect, they shall be immediately corrected with the recipient unless this is of no importance to the assessment of facts.

Part IV Final Provisions

Section 27. Applicability of the Federal Data Protection Act
Section 3, subsections 2 and 8, no. 1, section 4, subsections 2 and 3, sections 4b and 4c and sections 10 and 13 to 20 of the Federal Data Protection Act shall not apply to the fulfilment of the Federal Office for the Protection of the Constitution’s tasks as defined in section 3.

Act on the Federal Intelligence Service
(BND Act)

- Gesetz über den Bundesnachrichtendienst (BNDG) -

Section 1. Organization and functions
(1) The Federal Intelligence Service is a higher Federal authority within the remit of the Federal Chancellery. It must not be attached to a police authority.
(2) The Federal Intelligence Service shall collect and analyze information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of the Federal Republic of Germany. If within the scope of this Act information including personal data are collected for this purpose, their collection, processing and use shall be subject to Sections 2 to 6 and 8 to 11.

---

Section 2. Powers

(1) The Federal Intelligence Service may collect, process and use the required information, including personal data, in so far as this does not conflict with the applicable provisions of the Federal Data Protection Act or Special regulations in this Act,

1. for the protection of its staff members, facilities, objects and sources against sensitive or intelligence activities,
2. for the security screening of persons who work or are to work for it,
3. for the checking of information obtained, which is necessary for the Performance of functions, and
4. about events abroad which are important for the foreign and security policy of the Federal Republic of Germany, if such information can be obtained only in this way and no other authority is responsible for its collection.

(2) If personal data are collected with the knowledge of the data subject, the purpose of the collection shall be stated. The data subject shall be informed about the fact that he makes his statements on a voluntary basis and, in the case of a security screening pursuant to paragraph 1, no. 2, that he is obliged to cooperate in accordance with his contract of employment or other such agreements. In the case of security screenings, the Security Screening Act dated April 20, 1994 (Federal Law Gazette I, p. 867) shall be applied.

(3) The Federal Intelligence Service shall have neither police powers nor the power to give instructions. It must neither request the police by way of administrative assistance to take measures which it is not authorized to take on its own.

(4) Of several appropriate measures the Federal Intelligence Service shall select that one which will probably least affect the data subject. Any such measure must not lead to a disadvantage which is recognizably out of proportion to the intended result.

Section 2a. Special requests for information

Where necessary in individual cases in order to discharge the tasks of the Federal Intelligence Service pursuant to Section 1 (2), the Federal Intelligence Service may request information pursuant to Section 8a of the Federal Act on the Protection of the Constitution. Section 8a (2) of
the Federal Act on the Protection of the Constitution shall be applied subject to the proviso that concrete indications of a serious threat to the areas of danger stated in Section 5 (1), sentence 3, nos. 1 to 4 and 6 of the Article 10 Act shall apply instead of a serious threat to the protected interests stated in Section 3 (1) of the Federal Act on the Protection of the Constitution. Orders pursuant to Section 8a (2) of the Federal Act on the Protection of the Constitution may only be directed against persons who may be assumed to be involved in establishing or maintaining such a threat on the basis of concrete indications to this effect, and against persons specified in Section 8a (3), no. 2 of the Federal Act on the Protection of the Constitution. Section 8a (4) to (7) of the Federal Act on the Protection of the Constitution shall be applied subject to the proviso that the Federal Chancellery shall take the place of the Federal Ministry of the Interior and the federal ministry commissioned by the Federal Chancellor. The fundamental right of the privacy of correspondence, posts and telecommunications (Article 10 of the Basic Law) shall be curtailed to this extent.

**Section 3. Special forms of data collection**

The Federal Intelligence Service may for the clandestine collection of information, including personal data, apply the means pursuant to Section 8 (2) of the Federal Act on the Protection of the Constitution if there are facts justifying the assumption that this is necessary for the performance of its functions. Section 9 of the Federal Act on the Protection of the Constitution shall be applied mutatis mutandis.

**Section 4. Storage, modification and use of personal data**

(1) Pursuant to Section 10 of the Federal Act on the Protection of the Constitution, the Federal Intelligence Service may store, modify and use personal data in so far as this is necessary for the performance of its functions.

(2) The storage, modification and use of personal data on minors shall be admissible only in accordance with the provisions of Section 11 of the Federal Law on the Protection of the Constitution and where, according to the circumstances pertaining to the individual case concerned, it cannot be ruled out that the minor may constitute a threat to the life and limb of German nationals abroad or to German institutions

abroad.

Section 5. Correction, erasure and blocking of personal data

(1) The Federal Intelligence Service shall correct, erase and block the personal data stored in data files, pursuant to Section 12 of the Federal Act on the Protection of the Constitution, subject to the proviso that the checking period pursuant to Section 12 (3), sentence 1 of the Federal Act on the Protection of the Constitution shall have a duration of ten years.

(2) The Federal Intelligence Service shall correct and block personal data stored in records, pursuant to Section 13 of the Federal Act on the Protection of the Constitution.

Section 6. File directives

The Federal Intelligence Service shall issue a file directive for each automated file with personal data pursuant to Section 14 of the Federal Act on the Protection of the Constitution which shall require the approval of the Federal Chancellery. Section 14 (2) and (3) of the Federal Act on the Protection of the Constitution shall be applied.

Section 7. Information furnished to the data subject

The Federal Intelligence Service shall furnish the data subject at his request with information about personal data stored pursuant to Section 4 in accordance with Section 15 of the Federal Act on the Protection of the Constitution. The reference made there to the Ministry of the Interior shall be replaced by a reference to the Federal Chancellery.

Section 8. Communication of information to the Federal Intelligence Service

(1) The authorities of the Federation and the Federal institutions with legal personality governed by public law may on their own initiative communicate information, including personal data, having become known to them, to the Federal Intelligence Service if there are good grounds to suppose that the communication is required

1. for its own security pursuant to Section 2 (1), no. 1, or

2. within the framework of its functions pursuant to Section 1 (2) for the collection of information about the areas of danger mentioned
in Article 5 (1), sentence 3 of the Article 10 Act. Sentence 1, no. 2 shall apply to the Federal Ministry of Defence and the agencies of the Federal Armed Forces subject to the proviso that communication to the Federal Intelligence Service is necessary in discharging the tasks pursuant to Section 1 (2).

(2) The public prosecutors and, subject to the supervisory authority of the public prosecutors, the police, the agencies of the customs investigation service and other customs agencies, to the extent that these discharge functions according to the Act on the Federal Police, shall on their own initiative communicate information, including personal data, having become known to them, to the Federal Intelligence Service if there are good grounds requiring the communication for its own security pursuant to Section 2 (1), no. 1. Additionally, they may on their own initiative communicate information, including personal data, having become known to them, to the Federal Intelligence Service in accordance with paragraph 1, no. 2.

(3) Pursuant to Section 18 (3) of the Federal Act on the Protection of the Constitution, the Federal Intelligence Service may request every authority to communicate information, including personal data, required for the performance of its functions and, pursuant to Section 18 (4) of the Federal Act on the Protection of the Constitution, inspect official registers, in so far as this is necessary for the performance of its functions. Section 17 (1) and Section 18 (2) of the Federal Act on the Protection of the Constitution shall be applied.

(4) For the communication of personal data, which have become known on account of a measure pursuant to Section 100a of the Code of Criminal Procedure, Section 18 (6) of the Federal Act on the Protection of the Constitution shall be applied mutatis mutandis.

**Section 9. Communication of information by the Federal Intelligence Service**

(1) The Federal Intelligence Service may communicate information, including personal data, to domestic public bodies, if this is necessary for the performance of its functions, or if the recipient needs the data for purposes of public security. Unless the law provides otherwise, the recipient may use the data communicated only for the purpose for
which they were transmitted to him.

(2) Section 19 (2) to (5) of the Federal Act on the Protection of the Constitution shall be applied mutatis mutandis to the communication of information, including personal data, to other authorities; the communication pursuant to paragraph 4 of this provision shall be admissible only if it is necessary for safeguarding the foreign and security policy interests of the Federal Republic of Germany and the Federal Chancellery has given its consent. As regards personal data communicated by authorities for the protection of the constitution within the meaning of Section 18 (1a), sentence 1 of the Federal Act on the Protection of the Constitution, Section 18 (1a), sentences 2 to 4 of the Federal Act on the Protection of the Constitution shall apply mutatis mutandis.

(3) The Federal Intelligence Service shall communicate information, including personal data, to the public prosecutors, the police authorities and the Military Counterintelligence Service pursuant to Section 20 of the Federal Act on the Protection of the Constitution.

Section 9a. Project-related joint files

(1) The Federal Intelligence Service may set up a joint file for the duration of temporary project-related cooperation with the authorities of the Federation and the Federal States for the protection of the constitution, the Military Counter-Intelligence Service, the police authorities at Federation and Federal State level and the Central Office of the German Customs Investigation Service. In accordance with the remits and powers of the authorities stated in sentence 1, such project-related cooperation shall be aimed at exchanging and jointly evaluating information with regard to

1. the areas of danger stated in Section 5 (1), sentence 3, nos. 1 to 3 of the Article 10 Act or
2. the areas of danger stated in Section 5 (1), sentence 3, nos. 4 to 6 of the Article 10 Act insofar as the appurtenant intelligence operations entail links to international terrorism.

Personal data pertaining to the areas of danger pursuant to sentence 2 may be used via recourse to the joint file by the authorities involved in the project-related cooperation within the scope of their powers
where necessary in connection with discharging their tasks. The fur-
ther use of such personal data shall be subject to the provisions on the
use of data such as apply specifically to the respective authorities in-
volved.

(2) The entry of personal data in the joint file shall be subject to the pro-
visions on communication such as apply to the respective cooperating
authorities, with the proviso that entry shall be permissible only when
communication of the data to all authorities involved in the project-
related cooperation is permissible. Entry shall further only be permis-
sible when the authority entering the data is also permitted to store
the data in files of its own. The data shall be identified.

(3) A project-related joint file shall be kept subject to the provisions of
Sections 4 and 5 in conjunction with Section 6, sentences 5 to 7 and
Section 14 (2) of the Federal Act on the Protection of the Constitution.
Section 7 of this Act shall be applied subject to the proviso that the
Federal Intelligence Service shall issue the information in consulta-
tion with the authority bearing responsibility for data protection pur-
suant to sentence 1 and the participating authority concerned shall
verify the admissibility of issuing the information according to the
provisions to which it is subject.

(4) A joint file pursuant to sentence 1 shall be limited in duration to a
maximum of two years. The aforesaid period may be extended twice
by a further period of one year in each instance, if the objective of the
project-related cooperation has not yet been attained at the end of the
project and the file remains necessary for the purpose of attaining the
objective.

(5) The correction, blocking and erasure of data on a person by the au-
thority which has entered the data shall be subject mutatis mutandis
to the provisions on the correction, blocking and erasure of data
which are applicable to the authority concerned.

(6) For the joint file, the Federal Intelligence Service shall stipulate the
information pursuant to Section 6 in conjunction with Section 14 (1),
sentence 1, nos. 1 to 7 of the Federal Act on the Protection of the Con-
stitution in a directive on file management, together with the follow-
ing additional details and stipulations:
1. the legal basis for the file,
2. the type of personal data to be stored,
3. the type of personal data serving to render the file accessible,
4. conditions, subject to which data stored in the file may be transferred, further stipulating to whom such data may be communicated and according to which procedure,
5. in consultation with the authorities participating in the project-related cooperation, the latters’ organisational units which are authorised to enter and retrieve data,
6. immediate notification by the authorities sharing the joint file of the authority entering data in the case of indications that the entered data is incorrect, examination and, where necessary, prompt modification, correction or erasure of such data by the authorities which entered them,
7. the possibility of entering additional data to the data already stored on a person by the authorities sharing the joint file,
8. documentation of the time of retrieval, the necessary information to identify the retrieved data record and the authority responsible for retrieval, for each case of data retrieval from the joint file by the Federal Intelligence Service for the purposes of monitoring data protection, including specification of the purpose for which the documented data are to be used and their erasure deadline and
9. the responsibility of the Federal Intelligence Service for claims for compensation asserted by the data subject pursuant to Section 8 of the Federal Data Protection Act.

The directive on file management shall require the approval of the Federal Chancellery and the supreme Federal or Federal States authorities responsible for supervision of the cooperating authorities. The Federal Commissioner for Data Protection and Freedom of Information shall be consulted prior to issuing a directive on file management. Section 14 (3), first clause of the Federal Act on the Protection of the Constitution shall apply mutatis mutandis.

**Section 10. Procedural rules for the communication of information**

Sections 23 to 26 of the Federal Act on the Protection of the Constitution shall be applied mutatis mutandis for the communication of information pursuant to Sections 8 and 9.
Section 11. Scope of the Federal Data Protection Act
For the performance of functions of the Federal Intelligence Service, Section 3 (2) and (8), sentence 1, Section 4 (2) and (3), Sections 4b and 4c and Sections 10 and 13 of the Federal Data Protection Act shall not be applied.

Section 12. Obligation to report
The Federal Intelligence Service shall inform the Federal Chancellery about its activities. In addition, it shall also directly inform the federal ministries within the scope of their competencies; in this context, the communication of personal data shall also be admissible.

Act on the Military Counterintelligence Service (MAD Act)

- Gesetz über den Militärischen Abschirmdienst (MADG) -

Section 1. Purpose

(1) The purpose of the Military Counterintelligence Service of the Ministry of Defense is the collection and analysis of information, specifically of personal and pertinent data, intelligence and documents concerning

1. efforts directed against the free and democratic order, the existence or security of the federal government or one of the federal states,
2. activities within the purview of this act posing a threat to national security or espionage activities on behalf of a foreign power, provided these activities or efforts target personnel, agencies or installations of the area of responsibility of the Federal Ministry of Defense and are carried out by individuals who are members of, or employed by, the ministry and its agencies or are suspected of such actions. In addition, the Military Counterintelligence Service is responsible for collecting and analyzing information, specifically personal and pertinent data, intelligence and documents on the involvement of members of the area of responsibility of the Federal Ministry of Defense and in-
dividends employed by or designated for employment by this ministry, in acts and activities counter to the ideal of international understanding (Article 9, paragraph 2 of the Basic Law), and in particular counter to the idea of peaceful coexistence of nations (Article 26, paragraph 1 of the Basic Law). Section 4 of the Act on the Federal Office for the Protection of the Constitution applies.

(2) In assessing the security situation of
1. agencies and installations of the area of responsibility of the Federal Ministry of Defense,
2. and the agencies and installations of allied armed forces and international military headquarters if the Federal Republic of Germany has undertaken responsibilities in international agreements ensuring the security of these agencies and installations and if the assessment of the security situation has been delegated to the Military Counterintelligence Service in an agreement between the Federal Ministry of Defense and the responsible highest federal state authority,

the Military Counterintelligence Service is, moreover, charged with the analysis of information and intelligence on the efforts and activities cited in paragraph 1 targeting these agencies and installations, whether or not they are carried out or suspected to be carried out by individuals who are either members of, or employed in, the area of responsibility of the Federal Ministry of Defense.

(3) The Military Counterintelligence Service is involved in
1. security vetting procedures of individuals who are members of the area of responsibility of the Federal Ministry of Defense, are employed there or designated for employment there, and
   a) who are entrusted, for the public benefit, with sensitive facts, material or intelligence, who are to be entitled to access to such facts or will be able to gain access to them, or
   b) who are employed or will be employed in future in sensitive positions of the area of responsibility of the Federal Ministry of Defense;
2. technical security measures against unauthorized access carried out in the area of responsibility of the Federal Ministry of Defense to protect facts, material or intelligence which is deemed sensitive
for the public benefit.

The powers and responsibilities of the Military Counterintelligence Service concerning its involvement in security vetting in accordance with clause 1, number 1, letters a and b are laid down in the Security Clearance Check Act dated 20 April 1994 (Federal Law Gazette I, p. 867).

(4) The Military Counterintelligence Service may not be affiliated with any police authority.

(5) The Military Counterintelligence Service is bound by general laws and regulations (Article 20 of the Basic Law).

Section 2. Responsibility in Special Cases

(1) In continuance of its responsibilities in accordance with Section 1, paragraph 1, the Military Counterintelligence Service may, in individual cases in which this is imperative, carry out its responsibilities towards individuals who are not members of the area of responsibility of the Federal Ministry of Defense or employed there. This is only permitted

1. in dealing with the spouse, committed partner or fiancé(e) of an individual specified in Section 1, paragraph 1 or the person living in a quasi-marital relationship with him or her, if there are compelling grounds for assuming that he or she may be actively pursuing efforts or activities as specified in Section 1, paragraph 1;

2. in consultation with the responsible authority for the protection of the constitution in dealing with persons who provide actual grounds to suppose that they are cooperating with an individual as specified in Section 1, paragraph 1 in pursuing goals or activities as laid down in Section 1, paragraph 1, and if otherwise further investigations would be endangered or could only be pursued with inordinate effort.

(2) If it becomes imperative, in individual cases, to protect its staff, agencies, property and sources from espionage activities or activities posing a threat to national security, the Military Counterintelligence Service may, in carrying out its tasks in accordance with Section 1, paragraph 1 and in consultation with the responsible authority for the protection of the constitution, exercise its powers towards persons who
are not members of the area of responsibility of the Federal Ministry of Defense or employed there.

**Section 3. Cooperation with the Authorities for the Protection of the Constitution**

(1) The Military Counterintelligence and the authorities for the protection of the constitution cooperate in carrying out their respective tasks. Their cooperation includes mutual support and assistance.

(2) To carry on with its work as laid down in Section 3, paragraph 1 of the Federal Act on the Protection of the Constitution, an authority for the protection of the constitution may, in consultation with the Military Counterintelligence Service, extend its actions to individuals who are either members or employees of the area of responsibility of the Federal Ministry of Defense and fall under the jurisdiction of the Military Counterintelligence Service if the individual case makes such actions imperative. These actions are only permitted towards individuals who provide actual grounds to suppose that they are cooperating with an individual under jurisdiction of the authority for the protection of the constitution in pursuing goals or activities as specified in Section 3, paragraph 1 of the Federal Act on the Protection of the Constitution, and if otherwise further investigations would be endangered or could only be pursued with inordinate effort.

(3) The Military Counterintelligence Service and the Federal Office for the Protection of the Constitution shall keep each other informed in all matters required in carrying out their respective tasks.

**Section 4. Powers of the Military Counterintelligence Service**

(1) The Military Counterintelligence Service is empowered to collect, process and utilize the information and specifically personal data it requires for the exercise of its functions in accordance with Section 8, paragraphs 2, 4 and 5 of the Federal Act on the Protection of the Constitution unless the pertinent regulations of the Federal Data Protection Act or specialized provisions of this act prohibit it. The Service is not empowered to collect personal data to fulfill its functions in accordance with Section 1, paragraph 2. The provisions laid down in Section 8, paragraph 2, clauses 2 and 3 of the Federal Act on the Protection of the Constitution apply; approval of the administrative instruc-
tion is granted by the Federal Ministry of Defense.

(2) The Military Counterintelligence Service has no police powers or directive authority; it is not permitted to request the police to carry out measures generally or under the heading of administrative assistance that the service itself is not authorized to carry out.

**Section 4a. Special Requests for information**

Section 8a of the Federal Act on the Protection of the Constitution shall apply mutatis mutandis, the words „serious threats to the vested rights referred to in Section 3, paragraph 1 [of the Federal Act on the Protection of the Constitution]“ being replaced for the purposes of the present Act by the words „serious threats to the vested rights referred to in Section 1, paragraph 1 [of this Act]“ and the words „Federal Ministry of the Interior“ by the words „Federal Ministry of Defense“. The fundamental right of the privacy of correspondence, posts and telecommunications (Article 10 of the Basic Law) shall be curtailed to this extent.

**Section 5. Specialized Forms of Data Collection**

The Military Counterintelligence Service is authorized to collect data and specifically personal data in accordance with Section 9 of the Federal Data Protection Act insofar as this is necessary

1. for the performance of its functions in accordance with Section 1, paragraph 1 and Section 2, paragraph 1, and the research of the required sources for this task or
2. to protect staff, installations, property and sources of the Military Counterintelligence Service against activities posing a threat to national security or espionage activities, including those covered under Section 2, paragraph 2.

Section 9, paragraphs 2 through 4 of the Federal Act on the Protection of the Constitution apply mutatis mutandis.

**Section 6. Storage, Alteration and Utilization of Personal Data**

(1) The Military Counterintelligence Service is authorized to store, alter and utilize personal data in accordance with Section 10 of the Federal Act on the Protection of the Constitution to the extent required for the performance of its functions. Data collected and stored in accordance
with Section 1, paragraph 2 concerning individuals who are neither members nor employees of the area of responsibility of the Federal Ministry of Defense may not be utilized for other purposes than the ones laid down in the above mentioned clause unless their utilization is permitted under Section 1, paragraph 1 as well.

(2) Data on minors stored in computer files or document files will be reviewed after two years to ascertain whether or not they need to be retained, and will be erased after five years at the latest, unless new intelligence relating to activities as laid down in Section 1, paragraph 1 or Section 2 have come to light after the subject had attained his/her majority. This will not apply if the individual in question is subjected to an investigation in accordance with Section 1, paragraph 3. The storage of personal data on minors before completion of their 16th year in computer and document files on them is prohibited.

Section 7. Correction, Purging and Blocking of Personal Data

(1) The Military Counterintelligence Service is obliged to correct, purge and block the personal data stored in its files in accordance with the rules laid down in Section 12 of the Federal Act on the Protection of the Constitution.

(2) The Military Counterintelligence Service is obliged to correct and block personal data lodged in document files in accordance with the rules laid down in Section 13 of the Federal Act on the Protection of the Constitution.

Section 8. File Directives

For each individual automated file containing personal data, the Military Counterintelligence Service is obliged to generate a file directive in accordance with Section 14 of the Federal Act on the Protection of the Constitution. This file directive must be approved by the Federal Ministry of Defense. Section 14, paragraphs 2 and 3 of the Federal Act on the Protection of the Constitution apply.

Section 9. Information to the Subject

In accordance with Section 15 of the Federal Act on the Protection of the Constitution, the Military Counterintelligence Service will inform
the subject of the personal data stored on him/her. Instead of the Ministry of the Interior cited in the said Act, read the Federal Ministry of Defense.

Section 10. Transmission of Information to the Military Counterintelligence Service

(1) Federal agencies and legal entities under public law directly accountable to federal authorities will notify the Military Counterintelligence Service of their own accord of any facts that have come to their attention providing indications of activities posing a threat to national security or intelligence activities on behalf of a foreign power or efforts covered by the purview of this Act which, by the use of violence or preparations for acts of violence, are directed against the protected assets as enumerated in Section 1, paragraph 1, clause 1, number 1 and clause 2 of this Act, if actual indications exist that notification of the Service is necessary for the Service to perform its functions in accordance with Section 1, paragraphs 1 and 2.

(2) The Military Counterintelligence Service is authorized under Section 18, paragraph 3 of the Federal Act on the Protection of the Constitution to request any public authority to transmit data including personal data that it requires for the performance of its functions. As part of the performance of these functions and to find out whether an individual is a member or employee of the area of responsibility of the Federal Ministry of Defense, the Service is entitled to access the Federal Armed Forces Personnel Management and Information System to retrieve the last name, first name, previous names, date of birth, rank, unit designator, and end of military service of the subject. The Military Counterintelligence Service is accountable for each individual retrieval. The Federal Ministry of Defense will only review the retrieval of data if the situation warrants it. In a service regulation, the Ministry stipulates

1. the group of staff within the Military Counterintelligence Service entitled to retrieve data,
2. the procedure to be observed for retrieval,
3. the data to be entered singly or cumulatively for retrieval, to include search runs using incomplete data,
4. the restriction of the personal data records to be transmitted following a retrieval request to the minimum required for identification of the subject,
5. the deletion of the data transmitted upon retrieval request which are no longer needed, and
6. the logging of all retrieval procedures and monitoring of this procedure by the agency data protection commissioner.

The Federal Commissioner for Data Protection will be consulted prior to promulgation and possible amendment of the service regulation.

(3) If the transmission of information in accordance with paragraph 2, clause 1 might endanger the envisaged measures or might unduly infringe on the rights of the subject, the Military Counterintelligence Service is entitled to access public records in carrying out its functions as laid down in Section 1, paragraph 1, clause 1, number 2 and clause 2. This act of accessing public records must be authorized by the head of the authority or his deputy.

(4) Section 17, paragraph 1, as well as Section 18, paragraph 5 of the Federal Act on the Protection of the Constitution will apply mutatis mutandis.

Section 11. Transmission of Personal Data by the Military Counterintelligence Service

(1) The Military Counterintelligence Service is authorized to transmit personal data in accordance with Section 19 of the Federal Act on the Protection of the Constitution. In place of the Federal Ministry of the Interior, read the “Federal Ministry of Defense will approve the transmission of personal data”. Section 18, paragraph 1a, clause 2 through 4 of the Federal Act on the Protection of the Constitution will apply mutatis mutandis to personal data as defined in Section 18, paragraph 1a, clause 1 of said Act which is transmitted by the authorities for the protection of the constitution.

(2) In accordance with Section 20 of the Federal Act on the Protection of the Constitution the Military Counterintelligence Service will transmit information, to include personal data, to public prosecutors’ offices, police authorities and the Federal Intelligence Service.
Section 12. Procedural Regulations for the Transmission of Information
Sections 23 through 26 of the Federal Act on the Protection of the Constitution apply mutatis mutandis for the transmission of information as intended by this Act.

Section 13. Applicability of the Federal Data Protection Act
In carrying out its functions as laid down in Section 1, paragraphs 1 through 3, Section 2 und Section 14 of this Act, Section 3, paragraphs 2 and 8, clause 1, Section 4, paragraphs 2 and 3, Section 4b and 4c, Sections 10 and 13 through 20 of the Federal Data Protection Act will not apply.

Section 14. Special Foreign Assignments
(1) In the course of special foreign assignments of the Federal Armed Forces as stipulated in Section 62, paragraph 1 of the Legal Status of Military Personnel Act or in the course of humanitarian missions instructed by the Federal Ministry of Defense, the Military Counterintelligence Service will collect and analyze information, in particular personal data and pertinent information, intelligence and documents which are necessary to ensure the operational readiness of the forces or to protect the personnel, installations and agencies of the area of responsibility of the Federal Ministry of Defense. This information will be collected and analyzed on German soil and abroad, although in the latter case the information will only be collected and analyzed within military installations and agencies in which German troops are stationed or employed. In order to fulfill this task, information may also be requested from agencies and public authorities in the country of deployment. These provisions are without prejudice to Section 1, paragraph 2 of the Federal Intelligence Service Act.

(2) In addition, in the course of special foreign assignments, the Military Counterintelligence Service will analyze information in accordance with paragraph 1 analogue to Section 1, paragraph 2 concerning individuals or groups of individuals who are not members or employees of the area of responsibility of the Federal Ministry of Defense, if their activities or efforts target deployed personnel, installations or agencies of
the said area of responsibility. Paragraph 1, clauses 2 and 3 apply mutatis mutandis. If collecting the required information in accordance with clause 1 of this paragraph is necessary, the Military Counterintelligence Service will request the Federal Intelligence Service to carry out the necessary action.

(3) In the course of the Federal Armed Forces’ special foreign assignments as defined in paragraph 1, the Military Counterintelligence Service will also be involved in security vetting of personnel and physical security arrangements in accordance with Section 1, paragraph 3 in the country of Federal Armed Forces deployment. Paragraph 1, clauses 2 and 3 apply accordingly.

(4) Should it be necessary in performing functions in accordance with paragraphs 1 through 3 to collect information, including personal data, in Germany or on German citizens, collection, further processing and utilization of the information will be carried out as laid down in Sections 4 through 8 and 10 through 12. In foreign countries, special forms of information collection as laid down in Section 5 are absolutely prohibited outside military installations as defined in paragraph 1. Intelligence collection in Germany is only permitted following consultation with the cognizant authorities for the protection of the constitution and if otherwise further investigations would be endangered or could only be pursued with inordinate effort. Consultations may be arranged for a series of analogous cases.

(5) The tasks in accordance with paragraphs 1 through 3 and the attendant powers are limited in duration and physical scope by, among other things, the foreign assignment of the Federal Armed Forces itself.

(6) Notification of the Military Counterintelligence Service in accordance with Section 10, paragraph 1 refers to all information required by the Service for the performance of its functions as laid down in paragraphs 1 through 3. In order to do so, the Military Counterintelligence Service and the Federal Intelligence Service will cooperate within the framework of their legal obligations. The Military Counterintelligence Service and the Federal Intelligence Service will notify each other in all matters that either one or both need to have knowledge of to be able to perform their functions. Detailed arrangements of the coopera-
tion between the Military Counterintelligence Service and the Federal Intelligence Service in the course of special foreign assignments of the Federal Armed Forces or humanitarian missions will be agreed between the two services for each individual foreign assignment. The agreement will be approved by the Head of the Federal Chancellery and the Federal Minister of Defense; the Parliamentary Control Panel must be informed of the contents of the agreement.

(7) Prior to the Military Counterintelligence Service’s deployment on foreign assignment, the federal government will inform The Parliamentary Control Panel of this fact.