German Original translated by the European Parliament Translation Unit on behalf of Members of the European Parliament Marketa Gregorova, Mikulas Peksa and Martin Sonneborn.

Ministerial draft of the Federal Chancellery

Draft law amending the Federal Intelligence Service Act to implement the rulings of the Federal Constitutional Court and the Federal Administrative Court

A. Problem and objective

The Federal Constitutional Court, in its decision of 19 May 2020 – 1 BvR 2835/17 (Foreign-to-Foreign Telecommunications Surveillance by the Federal Intelligence Service), has declared §§ 6, 7 and 13 to 15 of the Federal Intelligence Service Act (BNDG) to be incompatible with Article 10(1) of the Basic Law (GG) and with Article 5(1) of the GG, and has set the legislator a deadline of 31 December 2021 at the latest for constitutionally compliant revision. The same applies to § 19(1) and § 24(1), first sentence, (2), first sentence and (3) of the BNDG insofar as they provide justification for the processing of personal data.

The statutory remit of the Federal Intelligence Service is to obtain information on foreign countries which is of foreign or security policy significance to the Federal Republic of Germany. In so doing, the Federal Intelligence Service makes a vital contribution to the security architecture of the Federal Republic of Germany.

Strategic telecommunications surveillance represents a substantial element of this work. It enables the Federal Intelligence Service to monitor current events in real time and inform political users and international partners about them.

Technical surveillance by intelligence services is gaining increasing significance in a globalised and technically interlinked world. If comprehensive surveillance of sources of threats is to be achieved, it is essential to the work of the Federal Intelligence Service to keep up with technical developments in an increasingly interlinked world. The forms of communication used are volatile and constantly changing.

When the Federal Intelligence Service Act was last amended in 2016, an attempt was made to respond to this development by creating more legally certain and specific norms.

While the Federal Intelligence Service previously based the performance of strategic foreign telecommunications surveillance solely on the statutory task allocation norm laid down in §1(2) BNDG, the most recent amendment clarified the legal position and special legal principles were established for strategic foreign telecommunications surveillance from within the country as well as for cooperation in this regard with foreign public agencies of other states. A special legal basis was created for the common holding of data with foreign public agencies.

By means of its judgment of 19 May 2020 (1 BvR 2835/17), the Federal Constitutional Court ruled for the first time that foreign nationals abroad can also invoke the protection afforded by Article 10(1) of the Basic Law and Article 5(1) of the Basic Law.

In order to respond to these rulings of the Federal Constitutional Court, the relevant norms of the Federal Intelligence Service Act must be thoroughly revised. Account should be taken of the vital role of effective foreign surveillance and, consequently, of the Federal Intelligence Service in the security architecture of the Federal Republic of Germany.

In its decision of 19 May 2020, the Federal Constitutional Court emphasises the paramount public interest in effective foreign surveillance (BVerfG 1 BvR 2835/17, para. 161). The provision of information to the Federal Government for its foreign and security policy decisions helps it to maintain its position in the power politics of international relations, and incorrect decisions with serious consequences can be averted (BVerfG, loc. cit., para. 162). On that basis, the Federal Constitutional Court takes the view that the issue is one of maintaining democratic self-determination while protecting the constitutional order; in other words, significant constitutional principles are involved. There is, therefore, a whole-state interest at stake which extends clearly beyond the importance of guaranteeing internal security as such (BVerfG, loc. cit., para. 162).

The Federal Constitutional Court also emphasises that threats from abroad have increased substantially in the wake of the development of information technology and international communications, and the greater ease of interaction between individuals across borders this has brought about. The early detection of threats from abroad is also, in the estimation of the Federal Constitutional Court, gaining particular significance for security. The expansion and internationalisation of communications options and the resulting increased politicisation and organisational capabilities of international criminal groups has given rise to dangerous situations in individual countries, often as a result of the activities of networks of actors cooperating internationally, which can quickly take on a foreign and security policy dimension. Such activities are partially aimed at destabilising society, and can pose a threat to the constitutional order, the continued existence and security of the federation or the *Länder*, and to life, limb and freedom. These are vitally important constitutional principles, and to protect them the legislator can regard foreign surveillance that is effective and, at the same time, circumscribed by the rule of law, as essential (BVerfG, loc. cit., para. 163).

The Federal Constitutional Court emphasises, further, that the far broader access to data granted to strategic surveillance authorities today must be seen in the context of the increase in security risks since the Federal Constitutional Court handed down its ruling in 1999. Above all, however, the Federal Constitutional Court emphasises that an important factor justifying strategic telecommunications surveillance is that the consequences are mitigated to some extent by its being undertaken by an authority which itself, in principle, does not have any operational powers (BVerfG, loc. cit., para. 164f.). As the data are collected by an authority which does not have operational powers of its own, further use of the data is initially conditional on independent screening. It is, therefore, only transfer of the data for operational use that must be secured by means of appropriate transfer thresholds (BVerfG, loc.cit., para. 165).

The Federal Constitutional Court makes clear, at the same time, that the powers concerning strategic surveillance, transfer of the data obtained and cooperation with foreign services in this area are consistent with the requirements of proportionality only if they are accompanied by independent oversight on the basis of objective law. This oversight is to be formulated as continuous legal oversight, which makes comprehensive oversight access possible. The Federal Constitutional Court demands, for this purpose, quasi-judicial oversight with final

decision-making powers, to which the essential procedural steps of strategic telecommunications surveillance are subject, as well as administrative oversight, by means of which the competent body can on its own initiative examine the legality of the entire process of strategic telecommunications surveillance on the basis of random samples (BVerfG, loc. cit., para. 272 et seq.). Institutionally independent oversight is to be guaranteed. This includes having a separate budget, independent recruitment powers and procedural autonomy. The oversight bodies are to be given the staff and resources they need to carry out their tasks effectively (BVerfG, loc. cit., para. 282 et seq.). They must have all the powers necessary for effective oversight of the Federal Intelligence Service, and that oversight must not be obstructed by the 'third-party rule' (BVerfG, loc. cit., para. 292 et seq.)

In addition to the decision of the Federal Constitutional Court, the amendment also implements the rulings contained in two decisions of the Federal Administrative Court of 13 December 2017 (BVerwG 6 A 6.19 and 6 A 7.16). In these proceedings the Federal Administrative Court was asked to rule on two actions brought against the traffic data analysis system used at that time by the Federal Intelligence Service (VERAS). Traffic data on communications by German nationals, domestic legal entities or persons resident on federal territory with other countries were stored in VERAS. However, before being stored the data were anonymised by the Federal Intelligence Service, so that the source could no longer be identified. The Federal Administrative Court viewed this as encroachment on the protection afforded by Article 10(1) of the Basic Law, in spite of the anonymisation undertaken prior to storage. Such interventions are thus permissible only if performed in accordance with a specific legal basis. However, this was lacking when the Federal Administrative Court handed down its ruling, both in the Federal Intelligence Service Act and in the Article 10 Act, and is now being created.

The objective of this fundamental amendment of the existing legal basis of the Federal Intelligence Service, in implementing the stipulations of the Federal Constitutional Court and the Federal Administrative Court, is thus to provide a more legally certain and specific legal basis for the work of the Federal Intelligence Service in the area of technical surveillance and the further processing of the data collected in this way. Foreign surveillance using technical resources which is effective and, at the same time, circumscribed by the rule of law is thus also to be made possible in the future.

B. Solution

The amendment of the Federal Intelligence Service Act leads to legally compliant formulation of the requirements arising out of the decision of the Federal Constitutional Court of 19 May 2020 (1 BvR 2835/17), implementing this decision and revising the Act in substantive and systematic respects. In addition, the amendment serves to implement two decisions of the Federal Administrative Court of 13 December 2017 (BVerwG 6 A 6.16 and 6 A 7.16).

C. Alternative

None.

D. Budgetary expenditure without compliance costs

[…]

E. Compliance costs

E.1 Compliance costs for citizens

There are no additional compliance costs for citizens.

E.2 Compliance costs for businesses

There are no compliance costs for businesses beyond those

they already incur.

E.3 Compliance costs for public authorities

[…]

F. Other costs

None.

Ministerial draft of the Federal Chancellery

Draft law amending the Federal Intelligence Service Act to implement rulings of the Federal Constitutional Court and the Federal Administrative Court

Of ...

The Bundestag has passed the following Act:

Article 1
Amendment of the Federal Intelligence Service Act

The Federal Intelligence Service Act of 20 December 1990 (Federal Law Gazette (BGBl.) I p. 2954, 2979), last amended by Article 19 of the Regulation of 19 June 2020 (BGBl. I p. 1328) shall be amended as follows:

1. In the title of Chapter 1, the words ‘of the Federal Intelligence Service’ shall be deleted.

2. In §1(2), second sentence, the words ‘under §§ 2 to 15, 19 to 21 and 23 to 32’ shall be replaced by the words ‘under the first sentence and §§ 2 to 8, 10 to 39, and 59 to 63’.

3. §3(3) shall be repealed.

4. §4, fourth sentence shall be repealed.

5. §5 shall be amended as follows:

   (a) In the first sentence, the words ‘the resources under §8(2) of the Federal Constitutional Protection Act’ shall be replaced by the words ‘intelligence resources’.

   (b) In the second sentence, the words ‘§§ 9, 9a and 9b’ shall be replaced by the words ‘§ 8(2) and §§ 9, 9a and 9b’.

   (c) The following sentence shall be added:

   ‘§ 1(2), first sentence, shall remain unchanged.’

6. In the title of Section 2, the words ‘foreign-to-foreign telecommunications surveillance’ shall be replaced by the words ‘further processing of data’.

7. §§ 6 to 18 shall be repealed.

8. The title of Section 3 shall be deleted.

9. The previous §§ 19 to 21 shall become §§ 6 to 8.

10. The previous § 22 shall become § 9, and in the first sentence ‘§ 19’ shall be replaced by ‘§ 6’.

11. The title of Section 4 shall be replaced by the following title:

‘Section 3
Transfer of data and shared files’.

12. The previous § 23 shall become § 10 and be amended as follows:

(a) In the title, the word ‘information’ shall be replaced by the words ‘personal data’.

(b) In paragraph (1), first sentence, the words ‘information including personal’ shall be replaced by the word ‘personal’.

(c) Paragraph (2) shall be amended as follows:

(aa) In the first sentence, the words ‘information including personal’ shall be replaced by the word ‘personal’.

(bb) In the second sentence, the words ‘information including personal’ shall be replaced by the word ‘personal’.

(d) In paragraph (3), first sentence, the words ‘information including personal’ shall be replaced by the word ‘personal’.

13. The previous § 24 shall become § 11 and be amended as follows:

(a) In the title, the word ‘information’ shall be replaced by the words ‘personal data’.

(b) Paragraph (1) shall be amended as follows:

(aa) In the first sentence, the words ‘information including’ shall be deleted and the word ‘personal’ [personenbezogener] shall be replaced by the word ‘personal’ [personenbezogene].

(bb) In the second sentence, the words ‘information including personal data’ shall be replaced by the words ‘personal data’.

(cc) In paragraph (2), first sentence, the words ‘information including personal’ shall be replaced by the word ‘personal’ and ‘§ 19(2) to (5)’ shall be replaced by the words ‘§ 19(3) to (5)’.

(c) In paragraph (3), the words ‘information including personal’ shall be replaced by the word ‘personal’.

14. The previous § 25 shall become § 12 and be amended as follows:

(a) Paragraph (1) shall be amended as follows:

(aa) In the first sentence, the words ‘and departments covered by the remit of the Ministry of Defence’ shall be inserted after the words ‘customs investigation office’.

(bb) The second sentence shall be amended as follows:

(aaa) In subparagraph 2, the full stop at the end shall be replaced by a comma.

(bbb) The following subparagraph 3 shall be inserted:

'3. protection of the functional capability of the Bundeswehr for national or alliance defence and protection of the functional capability of the Bundeswehr in international missions.'

(b) Paragraph (3) shall be amended as follows:

(aa) In the first sentence, the words 'through the Federal Intelligence Service'shall be inserted after the word 'file', and '§§ 19 and 20' shall be replaced by '§§ 6 and 7'.

(bb) In the second sentence, '§ 22' shall be replaced by '§ 9'.

(c) The following sentence shall be added to paragraph 4. 'If the objective of project-related cooperation under paragraph (1), second sentence, third subparagraph, relates to protection of the functional capability of the Bundeswehr in international missions and use of the file continues to be necessary to achieve this objective, the time limit may be extended beyond that laid down in the second sentence by one further year at a time, but not beyond the conclusion of the international mission.'

(d) Paragraph (6) shall be amended as follows:

(aa) In the first sentence, in the clause before the first subparagraph, the words 'if paragraph (3) applies' shall be inserted before the words 'for the common file' and '§ 21' shall be replaced by '§ 8'.

(bb) In the third sentence, the words 'The Federal Commissioner for Data Protection and Freedom of Information' [Der Bundesbeauftragte für Datenschutz] shall be replaced by the words 'The Federal Commissioner for Data Protection and Freedom of Information' [Die oder der Bundesbeauftragte für den Datenschutz].

15. The previous § 26 shall become § 13 and be amended as follows:

(a) In paragraph (1), first sentence, the words 'of intelligence service information and findings' shall be replaced by the words 'of personal data' and '(§ 27)' shall be replaced by '(§ 14)' and '(§ 30)' by '(§ 17)'.

(b) In paragraph 3, first sentence, the words 'of the European Economic Area' shall be replaced by the words 'of the European Free Trade Association'.

16. The previous § 27 shall become § 14 and be amended as follows:

(a) The words 'with foreign public agencies' shall be added to the title.

(b) In paragraph (1), first sentence the words '§ 26(1) as a separate file, these [...] on information and findings' shall be replaced by the words '§ 13(1) as a separate file, these]...] on personal data'.

17. The previous § 28 shall become §15, and the words ‘with foreign public agencies’ shall be added to the title.

18. The previous § 29 shall become § 16 and be amended as follows:

    (a) The words ‘with foreign public agencies’ shall be added to the title.

    (b) In paragraph (1), first sentence, the words ‘information including personal data’ shall be replaced by the words ‘personal data’, and the words ‘with foreign public agencies’ shall be inserted after the word ‘files’.

    (c) Paragraph (2), second sentence shall be amended as follows:

    ‘§ 32(4) and (8) and § 33(1) and (2) shall apply *mutatis mutandis*.’

    (d) In paragraph (4), the words ‘of controls on data processing including’ shall be inserted after the word ‘performance’.

19. The previous § 30 shall become § 17 and be amended as follows:

    (a) In the first sentence, ‘§ 26’ shall be replaced by ‘§ 13’.

    (b) In the second sentence, ‘§ 29’ shall be replaced by ‘§ 16’.

20. The previous § 31 shall become § 18 and be amended as follows:

    (a) In the title, the word ‘information’ shall be replaced by the words ‘personal data’.

    (b) The word ‘information’ shall be replaced by the words ‘personal data’ and ‘§ 23 and § 24’ by ‘§ 10 and § 11’.

21. The following Section 4 shall be inserted after the new § 18:

‘Section 4
Technical surveillance

Subsection 1
Processing of personal data in the course of strategic foreign telecommunications surveillance

§ 19
Strategic foreign communication surveillance

(1) The Federal Intelligence Service may, in carrying out its tasks, process using technical resources personal data of foreign nationals abroad on the basis of previously ordered strategic surveillance measures (strategic foreign telecommunications surveillance), insofar as this is necessary for the purposes of

1. political briefing of the Federal Government or of a *Land* government; or

2. early detection of foreign threats of international significance.

(2) A strategic surveillance measure shall restrict the objective of the strategic foreign telecommunications surveillance by specifying:

1. the purpose of the surveillance;

2. the topic of the surveillance;

3. the geographical focus; and

4. the duration.

(3) Strategic surveillance measures under paragraph (1), subparagraph 1, shall be permissible only if they serve to obtain information from abroad which is of foreign and security policy significance for the Federal Republic of Germany and for the surveillance of which the Federal Chancellery has issued an order to the Federal Intelligence Service.

(4) Strategic surveillance measures under paragraph (1), subparagraph 2, shall be permissible only if they serve to obtain information from abroad which is of foreign and security policy significance for the Federal Republic of Germany and for the surveillance of which the Federal Chancellery has issued an order to the Federal Intelligence Service, and there is actual evidence to suggest that information can be obtained:

1. with reference to the following sources of threats

   (a) national or alliance defence and missions carried out by the Bundeswehr (Federal Armed Forces) or allied armed forces abroad;

   (b) crisis-related developments abroad and their implications;

   (c) acts of terrorism or extremism whose perpetrators are prepared to use violence or are focused on the deliberately concealed imposition of political, religious or ideological views, or support thereof;

   (d) international criminal, terrorist or state-sponsored attacks by means of malware on the confidentiality, integrity or availability of IT systems;

   (e) organised crime;

   (f) international proliferation of weapons of war within the meaning of the War Weapons Control Act and highly significant cases of unlawful foreign trade in goods and technical support services;

   (g) critical infrastructure protection; or

   (h) hybrid threats;

2. relating to protection of the following legally protected interests:

   (a) the life, limb or freedom of a person;

   (b) continued existence or security of the Federal Government or a *Land*;

(c) continued existence or security of institutions of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation or continued existence or security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation; or

(d) ability of the Federal Republic of Germany to take foreign-policy action;

3. relating to the protection of essential public goods fundamental to human existence.

(5) The Federal Intelligence Service may collect personal data in the course of strategic foreign communications surveillance only through the use of search terms. These must be intended, suitable and necessary for the strategic surveillance measures under paragraph (1) and their use must be consistent with the foreign and security policy interests of the Federal Republic of Germany.

(6) Provided that it is necessary to carry out the strategic surveillance measures under paragraph (1), the Federal Intelligence Service may obtain access by technical means to information technology systems of a foreign telecommunications or telemedia service provider abroad, even without the latter's knowledge, and collect from the ongoing communications personal data which the latter processes in the course of providing its service. In so doing, the Federal Intelligence Service may also collect personal data which the foreign telecommunications or telemedia provider stores during its processing of ongoing communications in its information technology systems, provided that these are collected within the period covered by the order authorising the strategic surveillance measure under paragraph (1) and are not more than 48 hours old before they are collected by the Federal Intelligence Service. If the Federal Intelligence Service obtains access under the first sentence to an information technology system of a foreign telecommunication or telemedia provider abroad, it may also process inventory data of the foreign telecommunication or telemedia service provider which the latter processes in the course of providing its service, insofar as these are collected using search terms or relate to the counterpart of the recording made using the search term.

(7) Collection of the personal data of the following persons from telecommunications traffic shall not be permissible:

1. German nationals;

2. domestic legal entities; and

3. persons resident on federal territory.

Insofar as technically possible, automated filters shall be used to ensure that such data are filtered out. The data filtered out shall be erased automatically without undue delay. The filtering methods shall undergo continuous further development and kept consistent with the state of the art. If, despite this filtering, data are collected contrary to the first sentence, these data shall be erased without undue delay. This shall not apply if there is actual evidence that a significant threat to the life, limb or freedom of a person, the security of the Federal Government or a *Land* or the security of other Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation can be averted through further processing of the data. If the data are not erased without undue delay, the G10 Commission shall be briefed at its next meeting.

(8) Unrestricted strategic foreign telecommunications surveillance shall not be permissible. The volume of strategic foreign telecommunications surveillance shall be limited to not more than 30% of existing telecommunication networks.

(9) Strategic foreign telecommunications surveillance for the purpose of gaining competitive advantages (commercial espionage) shall not be permissible.

(10) Personal data shall be identified immediately after data collection as follows:

1. statement of the purpose of the data collection under paragraph (1); and

2. statement of the means used to collect the data.

Identification shall not be required in connection with transfers.

§ 20
Particular forms of strategic foreign telecommunications surveillance

(1) The targeted collection of personal data under §19(5) of institutions of the European Union, of public agencies of the Member States of the European Union or of Union citizens may take place only if it is necessary:

1. for early recognition of threats within the meaning of §19(4); or

2. for the gathering and evaluation of information within the meaning of §19(3), provided that only data on processes in third countries are to be obtained which are of particular foreign and security policy significance to the Federal Republic of Germany.

If it is subsequently recognised that such targeted data collection from institutions of the European Union, from public agencies of the Member States of the European Union or from Union citizens has taken place, further processing of the personal data may be carried out only if the conditions set out in the first sentence are met. They shall otherwise be erased without undue delay.

(2) The targeted collection of personal data of persons in respect of whom:

1. there is actual evidence that they are the source of threats within the meaning of § 19(4); and

2. transfer of the collected personal data is intended for the purposes of further processing for subsequent measures with direct external effect for the person concerned under subparagraph 1 in the area of threat aversion or criminal prosecution,

may be ordered only for early detection of threats (§ 19(1), subparagraph 2) under § 23(5), subparagraph 2, if special consideration was given in assessing proportionality to the increased probability of adverse consequences for these persons.

(3) Individualised monitoring of the entire telecommunications traffic of a person shall not be permissible.

§ 21
Protection of relationships of confidentiality

(1) The targeted collection of personal data under § 19(5) for the purpose of obtaining data covered by a relationship of confidentiality shall not be permissible. Relationships of confidentiality within the meaning of the first sentence shall be those of clergy, defence counsels, lawyers and journalists who would enjoy protection under § 53(1), first sentence, subparagraphs 1, 2, 3 and 5, and second sentence of the Code of Criminal Procedure.

(2) Notwithstanding paragraph (1), transfer shall be permissible if there is actual evidence to justify suspicion that

1. the person referred to in paragraph (1) is a perpetrator of or participant in the criminal offences referred to in § 29(3); or

2. this is necessary to avert a threat to:

   (a) the life, limb or freedom of a person;

   (b) essential public goods; or

   (c) the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

(3) If it is evident after further processing of the personal data that they are worthy of protection under paragraph (1), the data may be used only if the conditions set out in paragraph (2) are met. The data shall otherwise be erased without undue delay. The erasure shall be logged. Log data be used solely to perform oversight of data processing, including data protection control. Log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

§ 22
Core area protection

(1) Data collection for the purpose of obtaining information concerning the core area of private life shall not be permissible.

(2) If only further processing of the collected personal data reveals that these data fall within the core area of private life, they shall be erased without undue delay. The erasure shall be logged. Log data may be used only to perform data protection oversight. Log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

(3) If, in the course of further processing under paragraph 2, doubts arise and if the data are not to be erased without undue delay, the data may not undergo further processing without prior assessment by the Independent Oversight Council. If the Independent Oversight Council establishes that the data may not undergo further processing, the data shall be erased without undue delay. The erasure shall be logged. Log data may be used only to perform data

protection oversight. Log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

§23
Ordering measures

(1) Strategic surveillance measures under § 19(1) shall require an order by the President of the Federal Intelligence Service or his or her designated representative.

(2) The order under paragraph (1) shall be issued in writing. The order shall state:

1. the purpose for which intelligence is being gathered;

2. the topic of the surveillance within the meaning of § 19(3) or (4);

3. the geographical focus;

4. the duration;

5. a justification.

(3) In connection with strategic surveillance measures under § 19(1), subparagraph 2, the nature of the threat under § 19(4) which is the subject of the surveillance shall be specified in the presentation of the topic of surveillance.

(4) The Independent Oversight Council shall examine the legality of orders authorising strategic intelligence measures before they are implemented. If the Independent Oversight Council does not confirm the legality of an order, it shall cease to apply. Where there is an imminent threat, a provisional lawfulness assessment shall be carried out by a member of the Independent Oversight Council, if the intelligence purpose of the strategic intelligence measure would otherwise be thwarted or made substantially more difficult. If the provisional assessment establishes that the order is lawful, the latter may be put into effect. In that event, full assessment by the Independent Oversight Council shall be then performed without undue delay. If the Independent Oversight Council repeals the decision under the third sentence, the order shall cease to apply and data already collected shall be erased without undue delay.

(5) Targeted data collection under:

1. § 20(1), insofar as this relates to European Union bodies or to public agencies of its Member States;

2. § 20(2); and

3. § 21(2)

shall require an order by the President of the Federal Intelligence Service or his or her designated representative. If a restriction order under §§ 3, 5 or 8 of the Article 10 Act for the purposes stated in subparagraphs 1 to 3 has already been issued, no order under the first sentence shall be required. The Independent Oversight Council shall be briefed about corresponding restriction orders.

(6) The order under paragraph 5(1) shall be issued in writing. The order shall specify:

1. the strategic surveillance measure in the context of which the targeted data collection takes place;

2. the objective of the targeted data collection;

3. the duration of the targeted data collection;

4. a justification.

Specification of individual search terms to be used for targeted data collection shall not be necessary.

(7) The Independent Oversight Council shall assess the legality of orders authorising targeted data collection before they are implemented. If the Independent Oversight Council does not confirm the legality of an order, it shall cease to apply. Where there is an imminent threat, a provisional legality assessment shall be carried out by a member of the Independent Oversight Council, if the surveillance purpose of the targeted data collection would otherwise be thwarted or made substantially more difficult. Full assessment by the Independent Oversight Council shall then be performed without undue delay. If the provisional assessment establishes that the order is lawful, the latter may be put into effect. In that event, full assessment by the Independent Oversight Council shall then be performed without undue delay. If the Independent Oversight Council repeals the decision under the third sentence, the order shall cease to apply and data already collected shall be erased without undue delay.

(8) The Federal Intelligence Service shall inform the Federal Chancellery at regular intervals about orders issued under paragraphs (1) and (5).

§24
Suitability testing

(1) The Federal Intelligence Service may collect and evaluate personal data from telecommunications networks, provided that this is necessary to determine:

1. the suitability of telecommunication networks; or

2. the suitability of search terms in the context of strategic surveillance measures under § 19(1) (suitability testing).

(2) Suitability testing under paragraph 1, subparagraph 1, may be performed only if there is actual evidence that suitable data for strategic surveillance measures are transferred in the telecommunications network to be examined. A time limit of six months shall be set for the suitability testing under paragraph 1(1). Repeated six-month extensions shall be permitted.

(3) Suitability testing under paragraph 2, subparagraph 1, shall be ordered in writing by the President of the Federal Intelligence Service or his or her designated representative.

(4) If, for the performance of suitability testing, the involvement of an enterprise which provides commercial telecommunications services or is involved in the provision of such

services and has a registered office in Germany, or which provides or is involved in the provision of such services in Germany, is required, § 25 shall apply *mutatis mutandis*.

(5) The data collected in the course of a suitability test may be used only for the purpose of the suitability test itself. § 5(7) second to eighth sentences, of the Federal Office for Information Security Act shall apply *mutatis mutandis*. The Federal Intelligence Service may store the collected personal data, provided that this is necessary in order to carry out the suitability test. The evaluation shall be carried out without undue delay after collection.

(6) Personal data for the suitability test under paragraph (1), subparagraph 2, shall be erased no later than two weeks, and personal data for the suitability test under paragraph 1, subparagraph 1, no later than four weeks, after they have been collected. The first sentence shall not apply to personal data if their content at the time of collection can no longer be made readable for technical reasons and is needed for research purposes. Data of this kind collected in the course of the suitability test shall also be erased no later than after 10 years. The erasure shall be logged. Log data may be used only to perform oversight of data processing, including data protection oversight. Log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

(7) Notwithstanding paragraph (5), first sentence, it shall be permissible to

1. perform further processing of the personal data collected in the course of a suitability test if there is actual evidence that there is a significant threat to

    (a) the life, limb or freedom of a person;

    (b) the security of the Federal Government or a *Land* or the security of institutions of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation or of the Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation;

2. transfer of personal data collected in the course of a suitability test to the Bundeswehr, if there is actual evidence that this is necessary:

    (a) for the protection of the life, limb or freedom of a person;

    (b) for the protection of the functional capability of the Bundeswehr for national or alliance defence;

    (c) for the protection of the functional capability of the Bundeswehr in foreign missions; or

    (d) for the protection of the functional capability of the armed forces of the Member States of the European Union, the North Atlantic Treaty Organisation or the European Free Trade Association.

Transfer may also take place automatically in cases covered by the first sentence, subparagraph 2. The identification of data under § 19(10) shall not take place until further processing of the data is carried out under the first sentence.

§ 25
Duties of providers of telecommunications services, compensation

(1) Whosoever provides commercial telecommunications services or is involved in the provision of such services and has a registered office in Germany, or provides or is involved in the provision of such services in Germany, shall, on the order of the Federal Chancellery, provide information to the Federal Intelligence Service on the more detailed circumstances of the telecommunication carried out after the order becomes effective, hand over transmissions entrusted to it for transfer on the telecommunications route, and allow monitoring and recording of the telecommunication. §§ 3 and 4 shall not be affected. Whether and to what extent the telecommunications enterprise subject to obligation shall take precautions for technical and organisational implementation shall be determined under § 110 of the Telecommunications Act and the statutory regulation issued pursuant thereto.

(2) The order under paragraph (1), first sentence shall be issued in writing and shall be notified to the enterprise which has an obligation under paragraph (1) if this is necessary to enable it to fulfil its obligations. The order must specify:

1. the enterprise subject to obligation;

2. the duration of the obligation; and

3. the telecommunications concerned.

(3) The enterprise which has an obligation under paragraph 1 shall, before an intended measure is carried out:

1. select;

2. perform a simple security review on; and

3. inform the persons who are to be entrusted with carrying out the measure of notification bans under § 60 and the criminal nature of a breach under § 66; details of the manner of providing this information shall be placed on record.

Only persons who have been reviewed and informed pursuant to the first sentence may be entrusted with carrying out a measure. Once the Federal Chancellery has given its consent, the President of the Federal Intelligence Service or his or her designated representative may request in writing the enterprises which have an obligation under paragraph (1) to carry out the measure before the security review has concluded. Enterprises with an obligation under paragraph (1) shall ensure that the classification measures under the security classification order issued on 10 August 2018 by the Federal Ministry of the Interior, Building and Community (GMBl. 2018 No 44 – 47, p. 826) in the relevant version are taken.

(4) The security review under paragraph (3), first sentence, subparagraph 2, shall be carried out in accordance with the Security Review Act. The Federal Ministry of the Interior, Building and Community shall be responsible. If a person for whom an equivalent or higher security review in accordance with federal or *Land* law has already been performed is to be entrusted with carrying out a measure, no fresh security review shall be carried out.

(5) The Federal Intelligence Service shall agree compensation with the enterprises which have an obligation under paragraph 1 for the services referred to there, the level of which shall reflect the verified actual costs.

§ 26
Processing of personal traffic data

(1) The Federal Intelligence Service may also process traffic data in the context of strategic surveillance measures under § 19(1). § 19(6), first and second sentences, shall apply *mutatis mutandis*.

(2) Notwithstanding § 19(10), identification shall not take place until further processing of the data in the course of manual evaluation.

(3) Processing of personal traffic data of the following persons shall not be permissible:

1. German nationals;

2. domestic legal entities; and

3. persons resident on federal territory.

The first sentence shall not apply if:

1. only data which come to light in the course of automated information exchange between information technology systems without direct reference to a specific human communications process are processed; or

2. those traffic data which make it possible to identify the persons referred to in the first sentence are automatically masked without undue delay after they have been collected.

The automated masking under the second sentence of subparagraph 2 shall be performed in such a way that the clarity of the data is maintained and retroactive identification of the persons referred to in the first sentence is impossible or is only possible at unjustifiably high cost. The Federal Intelligence Service may further process traffic data which was masked under the second sentence of subparagraph 2 to fulfil its tasks, in order to:

1. identify persons outside the circle of persons referred to in the first sentence who have a connection to Germany and about whom information can be requested which is relevant to fulfilment of the task of the Federal Intelligence Service; and

2. determine suitable transmission routes within the meaning of § 10(4), second sentence, of the Article 10 Act.

(4) If only evaluation reveals that data contrary to paragraph (3), second sentence, subparagraph 2 were not masked, these data shall be masked without undue delay in accordance with paragraph (3), third sentence. If the data are not masked without undue delay, they shall be erased without undue delay. This shall not apply if there is actual evidence that a significant threat to the life, limb or freedom of a person, the security of the Federal Government or a *Land* or the security of other Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation can be

averted through further processing of the data. If the data are not masked or erased without undue delay, the G10 Commission shall be briefed at its next meeting.

(5) The traffic data shall be retained for a maximum of six months. Storage beyond that time limit shall be possible in an individual case if storage continues to be necessary to enable the Federal Intelligence Service to carry out its task. § 27 shall apply *mutatis mutandis* to further storage.

§ 27
Evaluation of data and assessment duties

The Federal Intelligence Service shall assess the personal data collected using search terms without undue delay and then at intervals of not more than seven years in order to determine whether, alone or together with data already available, they are necessary for the purposes referred to in § 19(1). Account shall be taken of the purpose of collection in each case in accordance with § 19(1). If the personal data are not necessary for these purposes, they shall be erased without undue delay. The erasure shall be logged. Log data

(1) may be used only to perform data processing oversight, including data protection oversight. Log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

(2) Data shall not be erased if they are necessary for a notification under § 59 or for oversight purposes of the Independent Oversight Council.

§ 28
Data collection by a foreign public agency

(1) The Federal Intelligence Service may request foreign public agencies to carry out strategic surveillance measures.

(2) The Federal Intelligence Service may process the data collected by the foreign public agency. The provisions set out in this subsection on data processing shall apply *mutatis mutandis*.

(3) If the foreign public agency uses search terms of the Federal Intelligence Service for data collection purposes, these search terms must fulfil the conditions laid down in § 19(5) and of §§ 20 to 22 and 23(5). The foreign public agency may use these search terms for its own purposes only after obtaining the prior consent of the Federal Intelligence Service. Such consent may be granted only if transfer of the search terms would be permissible under § 30.

Subsection 2
Transfer of personal data from strategic foreign telecommunications surveillance

§ 29
Transfer of personal data from strategic foreign telecommunications surveillance to domestic public agencies and other domestic entities

(1) The Federal Intelligence Service may transfer to the Federal Office for the Protection of the Constitution, the constitutional protection authorities of the *Länder* and to the Military Counterintelligence Service:

1. personal data identified for the purpose of early threat detection if there is actual evidence that this is necessary for the protection of particularly significant legal interests; and

2. personal data identified for the purpose of political briefing or of early threat detection, so that the Federal Government or a *Land* government can be informed if there is actual evidence that the transfer is necessary to fulfil their tasks or to fulfil the tasks of the recipients.

(2) The Federal Intelligence Service may transfer personal data identified for the purpose of political briefing or of early threat detection to other domestic public agencies so that the Federal Government or a *Land* government can be informed if there is actual evidence that the transfer is necessary to fulfil their tasks or to fulfil the tasks of the recipients.

(3) The Federal Intelligence Service may transfer data identified for the purpose of early threat detection to criminal prosecution authorities if there is evidence that this is necessary in order to prosecute:

1. criminal acts under § 100b(2) of the Code of Criminal Procedure; or

2. deliberate criminal acts under §§ 17 and 18 of the Foreign Trade and Payments Act.

(4) The Federal Intelligence Service may also transfer personal data identified for the purpose of early threat detection to the entities referred to in paragraph (2) for the purpose of further processing in preparation for follow-up measures with immediate external effect for the person concerned, in particular in order to avert threats:

1. insofar as this is provided for in other legal provisions; or

2. if there is actual evidence that this is necessary to avert a threat to particularly significant legal interests or to avert a particularly serious restriction of the rights of individuals.

(5) The Federal Intelligence Service may transfer data collected for the purpose of early threat detection to the Bundeswehr if there is actual evidence that this is necessary:

1. for the protection of the functional capability of the Bundeswehr for national or alliance defence and international missions;

2. for the protection of the functional capability of the armed forces of the Member States of the European Union, the North Atlantic Treaty Organisation or the European Free Trade Association;

3. for the protection of the life, limb or freedom of a person; or

4. for the protection of other particularly significant legal interests.

The Federal Intelligence Service may also transfer the personal data referred to in the first sentence provided that these were collected on the basis of search terms which are allocated to strategic surveillance measures under § 19(4), subparagraph 1(a) or subparagraph 2(a).

(6) The Federal Intelligence Service may transfer data collected for the purpose of early threat detection to other domestic entities if there is evidence that the transfer is necessary:

1. to protect the free, democratic order of society;

2. for the continued existence or security of the Federal Government or a *Land*; or

3. to guarantee the security of essential public goods, in particular for the protection of critical infrastructure.

Transfers under the first sentence shall require the prior consent of the Federal Chancellery. The Federal Intelligence Service may also transfer personal data to other domestic entities without the conditions set out in the first and second sentences being met if they are transferred solely to make an enquiry to another agency specifically and the data are already known to the latter.

(7) The Federal Intelligence Service may also transfer personal data identified for the purpose of political briefing of the Federal Government to domestic public agencies in circumstances not covered by paragraphs (1) and (2) if there is actual evidence that transfer is necessary to avert an imminent threat to:

1. the life, limb or freedom of a person;

2. essential public goods; or

3. the existence or security of the Federal Government or a *Land* or to the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

In cases covered by the first sentence, subparagraph 1, transfer to other domestic entities shall also be permissible in circumstances not covered by paragraph (6).

(8) Transfer of personal data from the relationship of confidentiality (§ 21(1), second sentence) shall be permissible. Notwithstanding the first sentence, transfer shall be permissible if there is actual evidence to justify suspicion that

1. the person referred to in § 21(1), second sentence is a perpetrator of or participant in the criminal offences referred to in paragraph (3); or

2. this is necessary to avert a threat to:

   (a) the life, limb or freedom of a person;

   (b) essential public goods; or

   (c) continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

(9) Transfer of personal data of minors below the age of 14 years may take place only if there is actual evidence that the minor is planning, is committing or has committed one of the crimes mentioned in § 3(1) of the Article 10 Act, or if, in the circumstances of the individual case, it cannot be ruled out that the minor poses a threat to the life or limb of German nationals abroad or to German institutions abroad. Transfer of personal data of minors aged 14 or over may take place only if it is necessary to avert a substantial threat or to prosecute a criminal offence of substantial significance.

(10) Transfer shall not take place if

1. it is apparent to the Federal Intelligence Service that, taking into account the nature of the information and its collection, the legitimate interests of the person concerned outweigh the public interest in transfer;

2. there are overwhelming opposing security interests; or

3. there are opposing statutory rules on further processing; the obligation to preserve confidentiality or professional and official secrets, which are not based upon statutory provisions, shall remain unchanged.

(11) The Federal Intelligence Service shall be responsible for the legality of transfer. If the transfer takes place at the request of a domestic public entity, the latter shall be responsible. In cases covered by the second sentence, the Federal Intelligence Service shall examine only whether the request for transfer falls within the tasks of the recipient, unless there is a particular reason for the legality of transfer to be examined.

(12) The Federal Intelligence Service shall refer the recipient to the purposes for which the data may be processed. The recipient may process the personal data solely for the purposes for which they have been transferred to it. The recipient shall be obliged to provide information to the Federal Intelligence Service on request. The attention of the recipient shall be drawn thereto on transfer. Further processing for other purposes shall not be permitted unless the conditions set out in paragraph (7) are met and the Federal Intelligence Service consents to the change of purpose. The Federal Intelligence Service may consent to a change of purpose, outwith the fifth sentence, of the data identified for the purpose of early identification of a threat at the request of the recipient if there is actual evidence that this change of purpose is necessary for the protection of comparably significant legal interests.

(13) The recipient shall examine whether the personal data transferred are necessary for fulfilment of its tasks. If the result of the examination is that they are not necessary, the recipient shall erase the data. Erasure may be omitted if it is not possible to separate other information necessary for fulfilment of the tasks or if it is only possible to do at excessive cost. In such a case, the processing of the data shall be restricted.

(14) If further personal data of the person concerned or of a third party are associated with personal data in documents in such a way that separation is not possible or is possible only at excessive cost, the transfer of these data shall also be permissible provided that legitimate interests of the person concerned or of a third party in confidentiality do not manifestly prevail. Further processing of these data shall not be permissible.

(15) If personal data prove to be incomplete or inaccurate, after being transferred, they shall be rectified without undue delay in relation to the recipient, unless this is of no significance to the assessment of the facts.

(16) The recipient, the legal basis of transfer and the time of transfer shall be logged. The log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

§ 30
Transfer of personal data from strategic foreign telecommunications surveillance to foreign public entities, supranational and intergovernmental entities and other foreign entities

(1) The Federal Intelligence Service may transfer the identified personal data for the purpose of political briefing or for the purpose of the early detection of danger to other domestic public entities for the purpose of briefing in the course of international political cooperation to foreign public entities and supranational and international entities if there is actual evidence that transfer is necessary for the fulfilment of its tasks.

(2) The Federal Intelligence Service may transfer the data identified for the purpose of the early detection of a threat to the entities referred to paragraph (1) if there is actual evidence that this is necessary to prosecute criminal offences which correspond to the criminal offences referred to in § 29(3). The provisions of the Act on International Mutual Assistance in Criminal Matters shall remain unchanged.

(3) The Federal Intelligence Service may also transfer the personal data identified for the purpose of the early detection of a threat to the entities referred to in paragraph (1) for the purpose of further processing for follow-up measures with immediate external effect for the person concerned, in particular in order to avert danger, if there is actual evidence that:

1. this is necessary to avert a threat to particularly weighty legal interests or a particularly serious adverse effect on the rights of individuals; or

2. transfer is necessary for the continued existence or security of the Federal Government or of a *Land*, to preserve substantial foreign policy interests of the Federal Government or of a *Land* or for the security of the recipient state.

(4) Transfer of personal data to other foreign entities shall be prohibited. Notwithstanding the first sentence, the Federal Intelligence Service may transfer the personal data collected in the course of strategic foreign telecommunications surveillance and identified for the purpose of the early detection of a threat to the entities referred to in the first sentence if there is actual evidence that the transfer is necessary to prevent an imminent threat to:

1. the life, limb or freedom of a person;

2. essential public goods; or

3. the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

Transfers under the second sentence shall require the prior consent of the Federal Chancellery. The Federal Intelligence Service may also transfer personal data to other foreign entities without the conditions set out in the second and third sentences being met if they are transferred solely in order to specify a request to another foreign entity and the data are already known to that other foreign entity.

(5) The Federal Intelligence Service may also transfer the personal data identified for the purpose of political notification of the Federal Government to the entities referred to in paragraph (1) outwith the first sentence of paragraph (1) if there is actual evidence that transfer is necessary to prevent an imminent threat to:

1. the life, limb or freedom of a person;

2. essential public goods; or

3. the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

In cases of the first sentence, subparagraph 1, transfer to other foreign entities shall also be permitted outwith paragraph (4).

(6) Transfer shall not take place if it is apparent to the Federal Intelligence Service that, taking into account the nature of the personal data and its collection, the legitimate interests of the person concerned prevail over the public interest in transfer. Legitimate interests of the person concerned shall prevail, in particular, if there is actual evidence that there is a danger that through the use of the transferred data substantial infringements of human rights or infringement of fundamental principles of the rule of law will occur, as in the case of use of the data for political persecution or for inhumane or demeaning punishment. In the event of doubt, the Federal Intelligence Service shall essentially take into account whether the recipient is given a binding assurance of appropriate protection of the transferred data and whether there is evidence that the assurance is not respected. The obligation to preserve confidentiality or professional and official secrets, which are not based upon statutory provisions, shall remain unchanged. Furthermore, transfer shall not take place if material security interests of the Federal Government or the *Länder* or material foreign policy interests of the Federal Republic of Germany would be adversely affected. In examining whether transfer shall not take place, the Federal Intelligence Service shall take account, in particular, of the nature of the information and its collection and the way in which the recipient has previously handled transferred data. The provisions of the Act on International Mutual Assistance in Criminal Matters shall remain unchanged.

(7) Personal data of minors below the age of 16 may not be transferred either to foreign to supranational and intergovernmental entities. Notwithstanding the first sentence, personal data on the behaviour of minors aged 14 or over may be transferred if, according to the circumstances in the individual case, it cannot be ruled out that the transfer is necessary to avert a substantial threat to life or limb of a person or there is actual evidence that the transfer is necessary for prosecution of one of the criminal offences referred to in § 3(1) of the Article 10 Act. Communication of personal data of minors aged 16 or over may take place only if it is necessary to avert a substantial threat or to prosecute a criminal offence of substantial significance.

(8) The Federal Intelligence Service shall be responsible for the legality of transfer. The recipient may process the transferred data solely for the purpose for which they have been transferred to it. Reference shall be made to the restriction of further processing and to the fact that the Federal Intelligence Service reserves the right to request information on the further processing of the data. Corresponding rights to information shall be agreed with the recipient. The latter must also give a binding assurance that any request from the Federal Intelligence Service for erasure will be acted upon. Transfer shall not take place if there is actual evidence that such an assurance is not respected by the recipient.

(9) § 29(8) and (13) to (16) shall apply *mutatis mutandis*.

Subsection 3
Cooperation in the course of strategic foreign telecommunications surveillance.

§ 31
Cooperation with foreign public entities

(1) If, in the course of strategic foreign telecommunications surveillance, the Federal Intelligence Service cooperates with foreign public entities which fulfil intelligence service tasks, personal data under §§ 32 and 33 may also be processed. Extension of the cooperation to data of the following persons shall not be permissible:

1. German nationals;

2. domestic legal entities and third persons resident on federal territory. § 19(7), first to fourth sentences shall be applicable.

(2) Strategic foreign telecommunications surveillance on the territory of the Federal Republic of Germany may take place in the course of such cooperation solely through the Federal Intelligence Service.

(3) Cooperation with the foreign public entities referred to in the first sentence of paragraph (1) shall be permissible for the early detection of substantial threats to the internal or external security of the Federal Republic of Germany, defence or common welfare, and in order to counter these dangers;

1. to preserve the foreign and security policy capability of the Federal Republic of Germany; or

2. to ensure that the Federal Intelligence Service can fulfil its role which, without such cooperation, is substantially more difficult or is impossible.

(4) Details of the operation shall be set out in writing before it begins in a declaration of intent between the Federal Intelligence Service and the foreign public entity. The declaration of intent shall record in particular:

1. the purpose of the cooperation;

2. the duration of the cooperation;

3. a binding assurance by the foreign public entity that:

(a) the data collected in the course of the cooperation are used solely for the purpose for which they were collected, and forwarding to third parties takes place only with the consent of the Federal Intelligence Service;

(b) data from telecommunication traffic of German nationals, of domestic legal entities or persons resident on Federal territory that were unintentionally processed contrary to the second sentence of paragraph (1) in conjunction with § 19(7) and are recognised as such by the foreign public entity in data evaluation are erased without undue delay;

(c) data of persons worthy of protection under the second sentence of § 21(1) that were unintentionally processed and are recognised as such by the foreign public entity in data evaluation shall be erased without undue delay;

(d) data concerning the core area of private life that were unintentionally processed and are recognised as such by the foreign public entity in data evaluation shall be erased without undue delay;

(e) the use of the data is consistent with the fundamental principles of the rule of law and the data in particular are used neither for political persecution nor for inhumane or demeaning punishment or treatment or for the suppression of opponents or particular population groups;

(f) the foreign public entity declares itself to be prepared, at the request of the Federal Intelligence Service, to issue information on the use made of the data;

(g) a request for erasure from the Federal Intelligence Service is acted upon;

(h) in the event of data transfer under § 33, the traffic data are not stored for a period of time longer than six months;

(5) The purpose of the cooperation must focus on obtaining information on:

1. the early detection of threats from international terrorism or extremism which is geared to the use of violence or is focused on the deliberately concealed imposition of political, religious or ideological views, or support thereof;

2. the early detection of threats from the illegal proliferation of weapons of mass destruction and war and from illegal foreign trade in goods and technical support services in cases of substantial significance;

3. protection of the Bundeswehr and the armed forces of the states taking part in the cooperation or the armed forces of the cooperating partners;

4. critical developments abroad and their implications;

5. the threat and security situation of German and foreign nationals;

6. political, economic or military processes abroad which are of substantial foreign and security policy significance;

7. intelligence and secret service activities with reference to the Federal Republic of Germany or the partner in cooperation;

8. international organised crime;

9. the establishment or maintenance of material capabilities of the Federal Intelligence Service or the partner in cooperation;

10. international criminal, terrorist or state-sponsored attacks by means of malware on the confidentiality, integrity or availability of IT systems; or

11. comparable cases.

(6) The objective of findings and the duration shall be set out in writing for individual cooperation purposes under paragraph (5). The objectives of findings shall not be opposed to the foreign and security policy interests of the Federal Republic of Germany.

(7) The declaration of intent shall require the consent of the Federal Chancellery if the cooperation takes place with foreign public entities of Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation. The declaration of interest shall, in addition, require the consent of the Head of the Federal Chancellery. The Parliamentary Oversight Panel shall be informed of the declaration of intent.

§ 32
Processing of selected personal data under cooperation

(1) The processing of selected personal data by the Federal Intelligence Service in the course of cooperation under § 31 shall be permitted:

1. in order to achieve the agreed purposes of cooperation; and

2. if, in collecting content data, only such search terms are used which are suitable for achieving the agreed purposes of cooperation. The collection of personal data and use of search terms must also be in harmony with the foreign and security policy interests of the Federal Republic of Germany. § 19(5), (7) and (9), § 20(1), § 21(1) and (2) and § 22(1) shall otherwise apply *mutatis mutandis*.

(2) The Federal Intelligence Service shall be responsible for the legality of the cooperation. If there is evidence that the partner in cooperation is not respecting the assurances given or agreements made, the Federal Intelligence Service shall work towards respect thereof and if necessary shall terminate the cooperation.

(3) Selected personal data may be collected under the cooperation if automated examination shows the permissibility of the search terms used. This permissibility shall exist if

1. the alignment of the search terms transferred by the partner in cooperation with the aims and contents of cooperation is shown to be plausible by the partner in cooperation; and

2. there is no actual evidence that

   (a) findings from the core area of private life are obtained by using the search terms; or

   (b) search terms of a person particularly needy of protection under § 21(1), second sentence are used.

(4) The data collected using the search terms under paragraph (3) may be transferred in an automated manner to the partner in cooperation in the course of the cooperation if the following data found in the course of automated examination were erased:

1. data under § 19(7) first sentence, transfer of which would be contrary to the national interests of the Federal Republic of Germany;

2. data belonging to the core area of private life; and

3. data which can be attributed to a person particularly needy of protection under § 21(1).

(5) The Federal Intelligence Service shall, using the results and experience from its work, collect any references to persons particularly needy of protection under § 21(1) and shall combine search terms to be allocated to these persons in order to be able to take account of the particular need to protect these persons. The databases and filtering methods in this regard shall be continuously updated and further developed.

(6) The transfer of the data shall be logged. The log data may be used solely to perform oversight of data processing, including data protection oversight, as well as to request erasure by the partner in cooperation under paragraph (7), third sentence. The log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

(7) Proper functioning of the automated examination under paragraphs (3) and (4) shall be reviewed on a random sample basis by the Federal Intelligence Service. The examination shall take place under the supervision of an official of the Federal Intelligence Service who is qualified for judicial office. If it is subsequently found that data were collected and transferred to the partner in cooperation contrary to these rulings, the partner shall be requested to erase the data. The Federal Intelligence Service shall inform the Federal Chancellery of performance of the examination under the first sentence at intervals of not more than six months.

(8) The data collected in the course of the cooperation on the basis of search terms nominated by the partner in cooperation shall be stored by the Federal Intelligence Service for the purpose of taking random samples under paragraph (7), first sentence and to determine new search terms under § 24(1)(2) for a period of two weeks.

§ 33
Processing of unselected traffic data under cooperation

(1) Automated transfer of unselected personal traffic data under a cooperation by the Federal Intelligence Service shall be permitted only if, in addition to the conditions under § 31 being met, there is a qualified need for surveillance.

(2) A qualified need for surveillance shall exist if the transfer of traffic data is necessary due to particular events, in order to counter specific threats or to ensure the capability of the Federal Republic of Germany or the partner in cooperation to act. These conditions shall be met, in particular, if there is actual evidence of:

1. the preparation of an armed attack on the Federal Republic of Germany or on Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation or on the partner in cooperation;

2. the preparation of acts of terror;

3. movements of weapons of war on a particular route or with a particular objective;

4. international criminal, terrorist or state-sponsored attacks by means of malware on the confidentiality, integrity or availability of IT systems;

5. surveillance of the working methods of other intelligence services with the aim of detecting state-controlled disinformation campaigns targeted at destabilisation with direct reference to the Federal Republic of Germany or with the aim of preparing or carrying out state-sponsored terrorist activities; or

6. preparations for an attack on such public legal interests whereby a threat affects the security or continued existence of the Federal Government or of a *Land* or the basis of existence of people.

The qualified need for surveillance shall be set out in writing and allocated to a strategic surveillance measure under § 19(1). The Independent Oversight Council shall examine the legality of the establishment of the qualified need for surveillance of the cooperation before data transfer is executed. If the Independent Oversight Council does not confirm that the establishment is lawful, the data transfer shall not take place.

(3) Cooperation under § 31 that covers the processing of unselected traffic data under paragraph (1) shall require approval by the President of the Federal Intelligence Service or a representative designated by the President of the Federal Intelligence Service.

Subsection 4
Particular forms of technical surveillance.

§ 34
Intervention in information technology systems of foreign nationals abroad

(1) The Federal Intelligence Service may, in order to fulfil its tasks, without the knowledge of the person concerned, intervene in information technology systems used by foreign nationals abroad on the basis of a previously ordered surveillance measure with technical resources and collected personal data including contents and circumstances of the ongoing communication stored on them, if this is necessary for the purpose of:

1. political briefing of the Federal Government or of a *Land* government; or

2. the early detection of impending dangers of international significance from abroad.

The individual surveillance measure may be carried out only if it is necessary for task fulfilment under § 1(2) and this would otherwise have no prospect of success or would be made substantially more difficult.

(2) An individual surveillance measure under paragraph (1), first sentence, subparagraph 1 shall be permitted only if there is actual evidence that it serves to obtain information, the surveillance of which the Federal Chancellery has charged the Federal Intelligence Service with and which are of substantial foreign or security policy significance for the Federal Republic of Germany.

(3) An individual surveillance measure under paragraph (1), first sentence, subparagraph 2 shall be permissible only if facts justify the assumption that findings will be obtained through it on dangers under § 19(4) in cases of elevated foreign and security policy significance for the Federal Republic of Germany.

(4) It shall be ensured technically that:

1. only changes which are essential for data collection are made to the information technology system; and

2. the changes made are reversed at the end of the measure and, as far as technically possible, in an automated manner.

The resource used shall be protected against unauthorised use according to the state of the art.

(5) The individual surveillance measure for the purpose of the early detection of a threat under paragraph (1), subparagraph 2 may be directed only against persons in relation to whom there is actual evidence that they:

1. pose threats within the meaning of §19(4); or

2. receive or pass on for the person posing a threat in accordance with subparagraph 1 particular information or information originating from him or the person posing a threat in accordance with subparagraph 1 uses their information technology system.

(6) An individual surveillance measure may also be carried out if other persons or information systems are unavoidably affected. In consideration of all existing findings, it shall not result in any disadvantage that is clearly disproportionate to the intended success. § 19(7) shall apply with the proviso that the briefing of the Independent Oversight Council shall take the place of the briefing of the G10 Commission and, in the cases of § 59(2), the decision of the Independent Oversight Council shall take the place of the decision of the G10 Commission.

(7) The Federal Intelligence Service shall examine without undue delay whether the personal data collected in the course of an individual surveillance measure under paragraph (1) is necessary alone or together with already existing data for the purposes under paragraph 1. With the consent of the Independent Oversight Council, notwithstanding the first sentence, an examination period of up to three years can be established in an individual case if examination without undue delay is not possible. If the data are not necessary for the purposes referred to in paragraph (1), they shall be erased without undue delay under the supervision of an official who is qualified for judicial office. The erasure shall be logged. The log data may be used solely to perform oversight of data processing, including data protection

oversight. The log data shall be erased at the end of the second calendar year following logging.

(8) Personal data shall be identified immediately after data collection as follows:

1. statement of the purpose of data collection under paragraph 1; and

2. statement of the means of data collection.

Identification shall not be applicable to transfers.

(9) Paragraph 7 shall apply *mutatis mutandis* to the evaluation of information technology systems of foreign nationals abroad that are in the possession of the Federal Intelligence Service or their depictions, with the proviso that evaluation must be carried out within three years of the data being made readable, unless the Independent Oversight Council consents to a longer time limit based on the circumstances in the individual case.

§ 35
Protection of relationships of confidentiality

(1) Individual surveillance measures under § 34(1) for the purpose of collecting personal data from a relationship of confidentiality (§21(1), second sentence) shall not be permissible.

(2) Notwithstanding paragraph (1), individual surveillance measures shall be permitted if there is actual evidence that:

1. the person referred to in § 21(1), second sentence is a perpetrator of or participant in one of the criminal offences referred to in § 29(3); or

2. this is necessary to prevent a threat to:

   (a) the life, limb or freedom of a person;

   (b) essential public goods; or

   (c) the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

(3) If it is evident only after processing of the data that these require protection under paragraph (1), the data may be used only if the conditions set out in paragraph (2) are met. The data shall otherwise be erased without undue delay. The erasure shall be logged. The log data may be used solely to perform the data protection oversight. The log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

§ 36
Protection of core area

(1) Data collection for the purpose of gaining knowledge of the core area of private life shall not be permissible.

(2) If it is not until further processing of the collected personal data has been performed that it is found that data were collected which fall within the core area of private life, they shall be erased without undue delay. The erasure shall be logged. The log data may be used solely to perform the data protection oversight. The log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

(3) If, in the course of further processing under paragraph (2), there are doubts and if the data are not to be erased immediately, the data may not undergo further processing without prior examination by the Independent Oversight Council. If the Independent Oversight Council establishes that the data may not undergo further processing, the data shall be erased immediately. The erasure shall be logged. The log data may be used solely to perform the data protection oversight. The log data shall be retained until the end of the second calendar year following logging and shall then be erased without undue delay.

§ 37
Orders

(1) Individual intelligence measures under § 34(1) shall require an order by the President of the Federal Intelligence Service or a representative who has been designated by the President of the Federal Intelligence Service. The Independent Oversight Council shall examine the lawfulness of the order before it is enforced. If the Independent Oversight Council does not confirm that the order is lawful, the order shall cease to be in force. Where there is an imminent threat, a provisional examination of lawfulness shall be made by a member of the Independent Oversight Council, if the surveillance purpose of the strategic surveillance measure would otherwise be thwarted or made substantially more difficult. If it is established in the provisional examination that the order is lawful, it may be put into effect. In this case, the examination by the Independent Oversight Council shall be obtained without undue delay. If the Independent Oversight Council repeals the decision under the fourth sentence, the order shall cease to be in force and data already collected shall be erased without undue delay.

(2) The order under paragraph (1) shall be issued in writing. It shall state:

1. the purpose of surveillance;

2. the surveillance topic pursued;

3. the objective of the individual surveillance measures;

4. the nature, extent and duration of the individual surveillance measure;

5. the justification; and

6. if necessary, the establishment of a longer period of examination under §34(7), second sentence or (9).

(3) The time limit of the order shall be set at not more than 12 months. Extensions of up to 12 months at a time shall be permitted provided that the conditions set out in the order

continue to be met in consideration of the findings obtained. If the conditions set out in the order are no longer met, the individual surveillance measure shall be terminated without undue delay.

(4) The Federal Intelligence Service shall inform the Federal Chancellery at regular intervals of orders under paragraph (1). The Federal Chancellery shall, in addition, inform the Parliamentary Oversight Body annually of the number of individual surveillance measures ordered.

§ 38
Transfer of personal data from individual surveillance measures to domestic public entities and other domestic entities

(1) The Federal Intelligence Service may transfer to the Federal Office for the Protection of the Constitution, the constitutional protection authorities of the *Länder* and the Military Counterintelligence Service:

1. the personal data identified for the purpose of the early detection of danger if there is actual evidence that this is necessary for the protection of particularly weighty legal interests; and

2. the personal data identified for the purpose of political notification or for the purpose of the early detection of a threat for the purpose of briefing the Federal Government or a *Land* government if there is actual evidence that the transfer is necessary to fulfil their tasks or to fulfil the tasks of the recipients.

(2) The Federal Intelligence Service may transfer the personal data identified for the purpose of political notification of the Federal Government or the government of a *Land* or for the purpose of the early detection of a threat to other domestic public entities for the purpose of briefing the Federal Government or a *Land* government if there is actual evidence that the transfer is necessary to fulfil their tasks or to fulfil the tasks of recipients.

(3) The Federal Intelligence Service may transfer the personal data identified for the purpose of the early detection of a threat to domestic criminal prosecution authorities if facts justify the assumption that this is necessary for the prosecution of a criminal offence under § 29(3).

(4) The Federal Intelligence Service may also transfer the personal data identified for the purpose of the early detection of a threat to the entities referred to in paragraph (2) for the purpose of further processing for follow-up measures with immediate external effect for the person concerned, in particular in order to avert danger if there is actual evidence that this is necessary to avert a threat to essential legal interests or to avert a particularly serious adverse effect on the rights of individuals.

(5) The Federal Intelligence Service may transfer the data collected for the purpose of the early detection of a threat to the Bundeswehr if there is evidence that this is necessary

1. for the protection of the functional capability of the Bundeswehr for national or alliance defence and in international missions;

2. for the protection of the functional capability of the armed forces of the Member States of the European Union, the North Atlantic Treaty Organisation or the European Free Trade Association;

3. for the protection of the life, limb or freedom of a person;

4. for the protection of legally protected interests of particular importance.

The Federal Intelligence Service may also transfer the personal data referred to in the first sentence provided that these were collected in the course of individual surveillance measures under § 34(1) with reference to the threats mentioned in § 19(4), subparagraph 1(a) or subparagraph 2(a).

(6) § 29(6) shall apply *mutatis mutandis* to transfers to other domestic entities.

(7) The Federal Intelligence Service may also transfer the personal data identified for the purpose of political briefing of the Federal Government to domestic public entities outwith paragraphs (1) and (2) if there is actual evidence that transfer is necessary to prevent an imminent threat to: the life, limb or freedom of a person;

2. essential public goods; or

3. the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

In cases of the first sentence, subparagraph 1, transfer to other domestic entities shall also be permissible outwith paragraph (6).

(8) § 29(8) to (16) shall otherwise apply *mutatis mutandis* to transfers under paragraphs (1) to (7).

§ 39
Transfer of personal data from strategic foreign telecommunications surveillance to foreign public entities, supranational and intergovernmental entities and to other foreign entities

(1) The Federal Intelligence Service may transfer the personal data identified for the purpose of political briefing of the Federal Government or a *Land* government or for the purpose of the early detection of a threat to other domestic public entities for the purpose of briefing in the course of international political cooperation of foreign public entities and supranational and intergovernmental entities if there is actual evidence that transfer is necessary for the fulfilment of its tasks.

(2) The Federal Intelligence Service may transfer the data identified for the purpose of the early detection of a threat to the entities referred to in paragraph (1) if there is actual evidence that this is necessary to prosecute criminal offences which correspond to the criminal offences referred to in § 29(3). The provisions of the Act on International Mutual Assistance in Criminal Matters shall remain unchanged.

(3) The Federal Intelligence Service may also transfer the personal data identified for the purpose of the early detection of a threat to the entities referred to in paragraph (1) for the

purpose of further processing for follow-up measures with immediate external effect for the person concerned, in particular in order to avert a threat, if it is to be assumed on the basis of particular facts that:

1. the data are of substantial significance for the recipient for the early detection of threats within the meaning of §19(4) or are necessary for the preservation of other substantial security interests; or

2. transfer is necessary to preserve substantial foreign and security policy interests of the Federal Government or a *Land*.

The decision on whether transfer is necessary shall be made under the supervision of an official of the Federal Intelligence Service who is qualified for judicial office.

(4) The Federal Intelligence Service may also transfer the personal data identified for the purpose of political notification to the entities referred to in paragraph (1) outwith paragraph (2) if there is actual evidence that transfer is necessary to prevent an imminent threat to:

1. the life, limb or freedom of a person;

2. essential public goods; or

3. the continued existence or security of the Federal Government or a *Land* or the security of a Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty Organisation.

(5) § 30(4) and (5), second sentence shall apply *mutatis mutandis* to transfers to other foreign entities.

(6) § 30(6) to (9) shall apply *mutatis mutandis* to transfers under paragraphs (1) to (5).

Subsection 5
Independent legal oversight

§ 40
Exercise of independent legal oversight

(1) The legality of technical surveillance and associated transfers and cooperation of the Federal Intelligence Service on the basis of the powers granted under this Act shall be subject to legal oversight by the Independent Oversight Council.

(2) Legal oversight shall be exercised as:

1. quasi-judicial legal oversight by the quasi-judicial oversight body; and

2. administrative legal oversight by the administrative oversight body.

§ 41
Independent Oversight Council

(1) The Independent Oversight Council shall be a supreme federal authority and, as an independent body for oversight of the technical surveillance of the Federal Intelligence Service, shall be subject only to the law.

(2) The Independent Oversight Council shall be chaired by a President. The President shall represent the authority externally. He or she shall direct the administration of the Independent Oversight Council and exercise administrative supervision.

(3) The Independent Oversight Council shall be independent and not bound by instructions in the exercise of it powers.

(4) The Independent Oversight Council shall be subject to examination of its budgetary and economic management by the Federal Audit Office, provided that its independence is not thereby adversely affected.

(5) The Independent Oversight Council shall, after consulting the Federal Chancellery, establish for itself:

1. internal regulations; and

2. rules of procedure.

Account shall be taken of the secrecy protection interests of the Federal Intelligence Service. The members of the quasi-judicial control body shall decide upon the internal regulations and rules of procedure by a majority of votes. If voting is tied, the President shall have the casting vote. The Independent Oversight Council shall inform the Parliamentary Oversight Body of its internal regulations.

(6) The offices of the Independent Oversight Council shall be located in Berlin and Pullach.

§ 42
Competence of the quasi-judicial oversight body

(1) The quasi-judicial oversight body shall be competent in the context of strategic foreign telecommunications surveillance for prior oversight of the legality of:

1. the ordering of strategic surveillance measures under § 23(1) (§ 23(4));

2. the ordering of objectives under § 23(5) (§ 23(7));

3. the establishment of a qualified need for surveillance in the processing of unselected traffic data in the course of cooperation of the Federal Intelligence Service with foreign intelligence services under § 33(2); and

4. the usability or erasure of data under § 22(3) in the event of doubt; and

5. the transfer of data under § 29(8) and § 30(9).

(2) The quasi-judicial oversight body shall further be competent in the context of strategic foreign telecommunications surveillance to monitor the legality of:

1. the use of data under § 21(3);

2. transfer under § 29(8) and § 30(9);

3. a change of purpose under § 29(7) and § 30(5);

4. the service regulations of the Federal Intelligence Service under § 62 insofar as they contain rules on the evaluation of data; and

5. the final decision on complaints of administrative legal oversight (§ 52(3)).

(3) The quasi-judicial oversight body is competent in the context of interventions into information technology systems of foreign nationals abroad under § 34 for the prior oversight of the legality of the ordering of individual surveillance measures under § 37(1) and the transfer of data under § 38(8) in conjunction with § 29(8) and § 39(6) in conjunction with § 30(9).

(4) The quasi-judicial oversight body shall, furthermore, be competent in the context of interventions in information technology systems of foreign nationals under § 34 for oversight of the legality of:

1. the use of data under § 35(3);

2. transfer under § 38(8) and § 39(6);

3. a change of use under § 38(7) and § 39(4); and 4. the final decision on complaints of administrative legal oversight (§ 52(3)).

§ 43
Composition of the quasi-judicial oversight body; Election of members

(1) The quasi-judicial oversight body of the Independent Oversight Council shall consist of six members, who prior to being nominated as members of the quasi-judicial oversight body were active as:

1. judges in the Federal Court of Justice (judicial members) with many years of experience in this activity; or

2. federal prosecutors under the Federal Public Prosecutor General of the Federal Court of Justice (public prosecutor members).

At least four members of the quasi-judicial oversight body must be judicial members. No more than two members may be state prosecutor members. The President of the Independent Oversight Council shall be the chair of the quasi-judicial oversight body.

(2) The members of the quasi-judicial oversight body shall undergo an expanded security review with security investigations under the Security Review Act,

The Parliamentary Oversight Panel shall select the members of the quasi-judicial oversight body on the basis of a proposal from the President of the Federal Court of Justice for the

judicial members and the Federal Public Prosecutor General at the Federal Court of Justice for the public prosecutor members by simple majority. The President or the

(3) Federal Public Prosecutor General shall notify the Federal Government, for information, of the proposal before the election.

§ 44
Legal position and nomination of the members of the quasi-judicial oversight body

(1) The members of the quasi-judicial oversight body shall be nominated as temporary civil servants. Subject to the rules set out in this Act, the provisions of the Federal Civil Service Act shall apply *mutatis mutandis*, with the exception of the provisions on careers and the period of probation. The members of the quasi-judicial oversight body shall be independent and subject only to the law.

(2) The Federal President shall nominate those elected under § 43(3).

(3) The members of the quasi-judicial oversight body shall pledge the following oath before the President of the German Bundestag: 'I swear that I will dedicate my efforts to the well-being of the German people, promote their welfare, protect them from harm, uphold and defend the Basic Law and the laws of the Federation, perform my duties conscientiously, and do justice to all. So help me God'. The oath may also be taken without religious affirmation.

(4) The members of the quasi-judicial oversight body shall bear the official designation of oversight officer in the Independent Oversight Council.

§ 45
Period of office of the members of the quasi-judicial oversight body

(1) The term of office shall be 12 years. Re-election shall not be permitted.

(2) The temporary status as civil servants for members of the quasi-judicial oversight body shall begin with the presentation of the certificate of appointment, unless a later date is specified in the certificate.

(3) On appointment as a temporary civil servant, the rights and duties arising from the position of civil servant or judge most recently transferred shall remain for the duration of the period of office. This shall not apply to the duty of confidentiality and the ban on accepting rewards, gifts and other benefits.

(4) The members of the quasi-judicial control body shall retire on expiry of the period of office, but no later than on reaching the age of 70. If the period of office of a judicial member in the Independent Oversight Council ends before the statutory standard retirement age under § 48(1) of the German Judges Act, he or she shall also be retired as a judge at the Federal Court of Justice at the time when his or her position as a member of the quasi-judicial oversight body ends, in accordance with § 45(1).

(5) The period of office under paragraph (1) shall be extended by the period until the election of a successor. Until that time, the members of the quasi-judicial control body shall continue with their official duties.

§ 46
Remuneration of the members of the quasi-judicial oversight body

(1) An official position in remuneration group B 7 shall be transferred to the members of the quasi-judicial oversight body from the start of the calendar month in which the position of temporary civil servant begins until the end of the calendar month in which it ends, in the case of § 45(5) until the end of the month in which the exercise of duties ends.

(2) Notwithstanding paragraph (1), an official position in remuneration group B 9 shall be transferred to the President of the Independent Oversight Council.

§ 47
Further rights and duties of the members of the quasi-judicial oversight body

(1) The provisions applicable to judges in the supreme federal courts on independence and disciplinary measures shall be applied *mutatis mutandis*. § 48(4) and (5) of the German Judges Act shall apply *mutatis mutandis*.

(2) The members of the quasi-judicial oversight body shall refrain from all actions not compatible with the tasks of their position. § 4 of the German Judges Act shall apply *mutatis mutandis*.

§ 48
Management of the Independent Oversight Council

The Parliamentary Control Body shall elect by simple majority, on the basis of a proposal from the Chair of the Parliamentary Control Body and from among the elected judicial members of the quasi-judicial control body, the President of the Independent Oversight Council and, from among the other members, the Vice-President. Notwithstanding § 44(4), those elected under the first sentence shall bear the official designation of President of the Independent Oversight Council and Director in the position of Vice-President of the Independent Oversight Council.

§ 49
Chamber of the quasi-judicial oversight body; Decision-making

(1) The members of the quasi-judicial oversight body shall form the Senate of the quasi-judicial oversight body. The Senate shall be chaired by the President. If the President is unable to attend, the Vice-President shall take the chair.

(1) The Senate of the quasi-judicial oversight body appoints two Chambers, each of which is composed of three members. The composition of a Chamber should not remain unchanged for longer than two years. Each Chamber appoints a Chair from among the judges-members.

(2) Judges-members must make up a majority of the judicial panels of the quasi-judicial oversight body.

(3) The Senate is quorate if a majority of its members are present and the majority are judges-members. The Chambers are quorate if a majority of their members are present. The judicial panels pass resolutions by a simple majority of the votes cast. In the event of a tie, the Chair has the casting vote. If the Chair is absent, the judge-member has the casting vote.

Section 50
Structure and organisation of the administrative oversight body

The administrative oversight body has a head. The head is qualified to hold judicial office. The head must be employed as a civil servant by the Federal Government and is assigned to grade B4. The head has the official title of director as head of the administrative oversight body. The head is bound by the President's instructions.

Section 51
Jurisdiction of the administrative oversight body

(1) The administrative oversight body supports the quasi-judicial oversight body in the exercise of the latter's oversight powers. In addition, it is competent to exercise legal oversight in the areas of technical intelligence gathering that are not subject to legal oversight by the quasi-judicial oversight body; in particular, if the primary competence of the quasi-judicial oversight body does not apply, it may review the legitimacy of search terms.

(2) The specific nature of the reviews carried out by the administrative oversight body are determined by the quasi-judicial oversight body at regular intervals. This does not affect the right of the quasi-judicial oversight body to issue orders to the administrative oversight body to carry out specific reviews in individual cases.

(3) The administrative oversight body has a right of objection pursuant to Section 52 within the framework of its oversight powers.

Section 52
Objections

(1) If the administrative oversight body identifies an irregularity while exercising its oversight powers, it may issue an objection concerning the Federal Intelligence Service. The administrative oversight body must consult the Federal Intelligence Service before the objection is issued.

(2) If the administrative oversight body issues an objection and if that objection is not remedied by an appropriate deadline set by the administrative oversight body, the administrative oversight body may refer the objection to the Federal Chancellery. The Federal Chancellery must issue an opinion on the objection.

(3) If the administrative oversight body upholds the objection even after the Federal Chancellery has issued its opinion, or if the Federal Chancellery does not issue an

opinion within three months of receiving the objection, the administrative oversight body may refer the objection to the quasi-judicial oversight body for a final decision.

(4) The quasi-judicial oversight body takes a decision on the objection after consulting the Federal Chancellery. If the quasi-judicial oversight body concludes that the objection is legitimate, it issues an order stating that the objection must be remedied immediately or by a deadline which it has set.

Section 53
Employees of the Independent Oversight Council

The employees of the Independent Oversight Council must be German nationals and must undergo an enhanced security clearance with security checks in accordance with the Security Clearances Act.

Section 54
Confidentiality; permission to give evidence

(1) The deliberations of the Independent Oversight Council are confidential.

(2) The members of the quasi-judicial oversight body and all employees of the Independent Oversight Council are obliged to maintain confidentiality in respect of matters disclosed to them during or in connection with their activities within the Independent Oversight Council. This obligation will continue to apply even after they have left the Independent Oversight Council.

(3) The President of the Independent Oversight Council decides whether permission to give evidence should be granted. Said permission must be refused if it would be detrimental to the interests of the Federal Government or a *Land* or if it would seriously jeopardise or significantly impede the performance of public tasks. The Vice-President decides whether permission to give evidence should be granted to the President.

Section 55
Reporting by the Independent Oversight Council

(1) The Independent Oversight Council reports on its work to the Parliamentary Oversight Panel at intervals of no more than six months.

(2) The reports pursuant to paragraph 1 are made after consulting the Federal Chancellery, with due regard for confidentiality, and are restricted to the information and topics covered by the discretionary powers of the Federal Intelligence Service. In other cases, the Federal Chancellery must inform the Independent Oversight Council. At the request of the Independent Oversight Council, the Federal Chancellery must take appropriate measures to ensure that reports on the above-mentioned information and topics can be submitted to the Parliamentary Oversight Panel. If necessary in keeping with the interests of the Federal Government or a *Land*, and in particular on compelling grounds relating to access to intelligence or the protection of third-party rights to

privacy, or if the matter relates to the core area of executive self-responsibility, the Federal Chancellery may refuse to approve the reports pursuant to paragraph 1. If the Federal Chancellery exercises this right, it must give the Independent Oversight Council its reasons for doing so.

(3) With due regard for confidentiality in an abstract sense, and after consulting the Federal Chancellery, the Independent Oversight Council may report objections to the German Bundestag. The Federal Chancellery may attach an opinion.

Section 56
Obligation of the Federal Intelligence Service to provide assistance

(1) The Federal Intelligence Service must assist the Independent Oversight Council with its tasks.

(2) Within the limits of its oversight powers, the Independent Oversight Council may request from the Federal Intelligence Service files or other documents that body holds if there is a justified interest in doing so in the specific case in question; it may also request the originals of those files or documents, and data stored in files.

(3) The Independent Oversight Council must at all times be granted:
1. access to all offices, and
2. access to all IT systems,

in so far as the Federal Intelligence Service has sole authority over those offices or systems and in so far as this is necessary to exercise oversight.

(4) The Independent Oversight Council may interview employees of the Federal Intelligence Service or obtain written information from them. Employees of the Federal Intelligence Service are obliged to provide complete and accurate information.

(5) The Federal Intelligence Service must comply immediately with requests made by the Independent Oversight Council pursuant to paragraph 4.

Section 57
Staff and facilities; human resources administration

(1) The Independent Oversight Council must be provided with the staff and facilities it needs to perform its tasks.

(2) The Independent Oversight Council may transfer tasks relating to human resources administration and human resources management to the Federal Chancellery provided that this does not undermine the independence of the Independent Oversight Council. Employees' personal data may be forwarded to those bodies if access to that data is necessary to perform the tasks transferred.

Section 58
Cooperation with the Parliamentary Oversight Panel, the G 10 Commission and the Federal Commissioner for Data Protection and Freedom of Information

(1) The Independent Oversight Council, the Parliamentary Oversight Panel, the G 10 Commission and the Federal Commissioner for Data Protection and Freedom of Information may exchange information on a regular basis concerning general matters relating to their oversight activities, provided that the respective confidentiality rules applicable in connection with the exercise of their individual oversight powers are observed.

(2) The Independent Oversight Council's activities do not affect the rights of the Parliamentary Oversight Panel to exercise oversight of the Federal Government in respect of the Federal Intelligence Service's activities. The Independent Oversight Council's activities do not affect the rights of the G 10 Commission and the Federal Commissioner for Data Protection and Freedom of Information to exercise oversight of the Federal Intelligence Service's activities.

Subsection 6
Notifications and evaluation

Section 59
Notification of data subjects and notification obligations

(1) If personal data of foreign nationals are collected abroad, the data subjects are not notified.

(2) If data are collected by way of derogation from Section 19(7), sentence 1, and if the data are not immediately erased pursuant to Section 19(7), sentence 5, the G 10 Commission must be notified thereof at its next meeting, and the data subject must be notified of the collection of the data, provided that:

1. the possibility that this might jeopardise the purpose of the measure has been ruled out, and
2. there is no likelihood that it will be to the overriding detriment of the interests of the Federal Government or a *Land*.

If notification is not effected within 12 months of the data being collected, further postponement of the notification must be approved by the G 10 Commission. The G 10 Commission determines the further duration of the postponement. Five years after collection of the data, with the approval of the G 10 Commission, a final decision against notification may be taken if it can be stated with a probability bordering on certainty that the requirements for such notification will not be met in the future. If the personal data may be relevant to a notification or a judicial review of the data collection, the erasure is postponed and restrictions are placed on the processing of the personal data; they may then only be used for that purpose.

Section 60
Ban on notifications

(1) Individuals who provide telecommunications or telemedia services or are involved in the provision of such services are obliged to maintain confidentiality in respect of the orders issued to them and their implementation pursuant to Section 25.

(2) If information is requested or issued pursuant to Section 25(1), sentence 1, inter alia in conjunction with Section 24(4), that fact or the content of the request or the information issued by individuals who are obliged to respond, entrusted with a response or involved in providing a response may not be disclosed to others.

Section 61
Evaluation

The Independent Oversight Council produces a report every five years evaluating the effectiveness of its oversight activities, and forwards that report to the Parliamentary Oversight Panel. The Federal Chancellery must first be given an opportunity to issue an opinion on the report.

Section 62
Service regulations

The technical and organisational arrangements for implementing the provisions on technical intelligence gathering must be outlined in service regulations. The service regulations must be approved by the Federal Chancellery. The Federal Chancellery must notify the Parliamentary Oversight Panel.'

22. The former Section 32 becomes Section 63.

23. The former Section 32a becomes Section 64, and '49, 50' is inserted in subparagraph 2 after '46'.

24. The former Section 33 becomes Section 65 and is reworded as follows:

'Section 65
Reporting obligation and provision of information to the public

(1) The Federal Intelligence Service reports directly to the Federal Chancellery and to the federal ministries within the scope of their remits; the forwarding of personal data is also permitted in that connection. Sections 11, 29 and 38 apply.

(2) The Federal Intelligence Service may provide the public with information about findings made in performance of its tasks pursuant to Section 1(2) or obtained when reappraising its records. When providing the information, it may also disclose personal data if:

1. said disclosure is necessary in order to understand the context or the description of organised or non-organised groups, and
2. the public interest outweighs the protected interest of the data subject.'

25. The former Section 34 becomes Section 66 and 'Section 17' is replaced by 'Section 59(2)'.

26. The former Section 35 becomes Section 67 and paragraph 1 is amended as follows:

a) In paragraph 1, ‘Section 8(1), sentence 1, or Section 8(2), sentence 3’ is replaced by ‘Section 25(1), sentence 1, or Section 25(3), sentence 3’.
b) In paragraph 2, ‘Section 8(2), sentence 2’ is replaced by ‘Section 25(3), sentence 2’.

27. The former Section 36 is replaced by the following Sections 68 and 69:

‘Section 68
Restriction of basic rights

The basic right to confidentiality of correspondence, post and telecommunications (Article 10 of the Basic Law) and the basic right to inviolability of the home (Article 13 of the Basic Law) are restricted by this Act.

Section 69
Transitional provisions

(1) Technical intelligence-gathering measures within the meaning of Section 4 that commenced prior to 1 January 2022 may continue until 31 December 2022. Those measures are subject to legal oversight by the administrative oversight body. Section 51 applies *mutatis mutandis*. If the measure is ordered for the first time pursuant to Section 23(1) or (5) or Section 37(1), and if the quasi-judicial oversight body does not confirm the lawfulness of the order, the measure must be discontinued immediately.

(2) The storage of data collected prior to 1 January 2022 and the storage of data collected on the basis of a measure pursuant to paragraph 1 is determined on the basis of Sections 18 and 19 in the version applicable on 19 June 2020.

(3) The transfer of data collected prior to 1 January 2022 and the transfer of data collected on the basis of a measure pursuant to paragraph 1 is determined on the basis of Section 23 in the version applicable on 19 June 2020.

(4) Until the technical requirements for identification provided for in Section 19(10), sentence 1, and Section 34(8), sentence 1, have been met, further processing of the personal data collected pursuant to Section 4 in the existing systems of the Federal Intelligence Service is permitted even without identification if the purpose and means of the data collection are otherwise traceable for data collected from 1 January 2022 onwards. Further processing within the structured databases of the Federal Intelligence Service is also permitted until the technical requirements for identification of the purpose and means have been met, even if the purpose and means of data collection are not otherwise traceable for each data field; in that respect those data are forwarded pursuant to paragraph 3. The Federal Chancellery submits an annual progress report to the Parliamentary Oversight Panel on the extent to which the technical requirements for identification pursuant to sentence 2 have been met.

(5) Cooperation agreements with foreign public agencies that are in force on 1 January 2022 pursuant to Section 13 of the version in force on 19 June 2020 will apply until 31 December 2024 at the latest.'

Article 2 Amendments to the Article 10 Act

The Article 10 Act of 26 June 2001 (Federal Law Gazette *(BGBl.)* I p. 1254, 2298; 2007 I p. 154), most recently amended by Article 38 of the Regulation of 19 June 2020 (*BGBl.* I p. 1328) is amended as follows:

1. The following Section 4a is inserted after Section 4:

‘Section 4a
Further processing of traffic data by the Federal Intelligence Service

(1) Further processing by the Federal Intelligence Service, in performance of its tasks, of traffic data which have been collected, and in respect of which a restriction relating to an individual involved in the communications has been ordered pursuant to Section 3, is permitted in order to:

1. identify individuals with a connection to Germany about whom information can be obtained that is relevant for the performance of tasks by the Federal Intelligence Service, or
2. identify suitable transmission routes within the meaning of Section 10(4), sentence 2.

(2) No later than three months after their collection, the traffic data stored pursuant to paragraph 1 must be reviewed to determine whether further storage is necessary for the performance of tasks by the Federal Intelligence Service. No later than six months after their collection, those data must be erased unless it has been decided in the specific case in question that further storage is necessary for the purposes outlined in paragraph 1. If it has been decided in the specific case in question that further storage is necessary for the purposes outlined in paragraph 1, the Federal Intelligence Service must carry out regular checks at intervals of no more than six months to determine whether the further storage of traffic data for those purposes is still necessary.

(3) Compliance with the requirements referred to in paragraphs 1 and 2 is checked on a regular and random basis by an authorised official of the Federal Intelligence Service who is qualified to hold judicial office. If the check reveals that the data have been processed unlawfully, the data must be erased immediately under the supervision of an official of the Federal Intelligence Service who is qualified to hold judicial office. Section 4(1), sentences 3 to 5, applies *mutatis mutandis*.’

2. Section 6 is amended as follows:

a) In paragraph 1 sentence 4, the words ‘for the purpose of data protection oversight’ are replaced by the words ‘for the purpose of overseeing data processing, including data protection oversight.’
b) In paragraph 3 sentence 5, the words ‘for the purpose of data protection oversight’ are replaced by the words ‘for the purpose of overseeing data processing, including data protection oversight.’
c) The following paragraphs 4 to 6 are added: ‘(4) Notwithstanding paragraph 1, sentences 1 and 2, the Federal Intelligence Service may also, in performance of its tasks, collect traffic data and process them further in keeping with the

requirements of sentence 3 using the transmission routes pursuant to Section 5(1) in conjunction with Section 10(4), sentence 2, if those traffic data make it possible to identify German nationals, domestic legal entities or persons present on the territory of the Federal Republic of Germany and are automatically rendered unidentifiable as soon as they are collected. The automated procedure to render the data unidentifiable must be carried out in such a way that:

1. the uniqueness of the data continues to be guaranteed, and
2. retroactive identification of the individuals referred to in sentence 1 is impossible or only possible on the basis of disproportionate effort. The Federal Intelligence Service may, in performance of its tasks, process traffic data that have been rendered unidentifiable pursuant to sentences 1 or 2 in order to:

1. identify individuals with a connection to Germany about whom information can be obtained that is relevant for the performance of tasks by the Federal Intelligence Service, with the exception of the group of individuals referred to in sentence 1, and
2. identify suitable transmission routes within the meaning of Section 10(4), sentence 2.

No later than six months after their collection, the traffic data referred to in sentence 1 must be erased unless it has been determined in the specific case in question that further storage is necessary for the purposes outlined in sentence 3. If it has been decided in the specific case in question that further storage is necessary for the purposes outlined in sentence 3, the Federal Intelligence Service must carry out regular checks when processing individual cases and after specified deadlines, at the latest after 10 years, to determine whether the traffic data that have been rendered unidentifiable are still required for those purposes.

(5) Notwithstanding paragraph 1, sentences 1 and 2, the Federal Intelligence Service may, in performance of its tasks, process traffic data that have been collected and captured on the basis of a search term pursuant to Section 5(2) in order to

1. identify individuals with a connection to Germany about whom information can be obtained that is relevant for the performance of tasks by the Federal Intelligence Service, and
2. determine suitable transmission routes within the meaning of Section 10(4), sentence 2.

If it is determined during further processing pursuant to sentence 1 that additional further processing of the traffic data by the Federal Intelligence Service is necessary in order to identify offences within the meaning of Section 3(1) or threats within the meaning of Section 5(1), sentence 3, or Section 8(1) and to respond to such threats, the further processing of those data by Federal Intelligence Service for such purposes is also permitted.

No later than three months after their collection, the traffic data referred to in sentences 1 and 2 must be reviewed to determine whether further storage is necessary for the performance of tasks by the Federal Intelligence Service. No later than six months after their collection, the data referred to in sentences 1 and 2 must be erased unless it has been determined in the specific case in question that further storage is necessary for the purposes outlined in sentences 1 and 2. If

it has been determined in the specific case in question that further storage is necessary for the purposes outlined in sentences 1 and 2, the Federal Intelligence Service must carry out regular checks at intervals of no more than six months, to determine whether the further storage of traffic data for the purposes outlined in sentences 1 and 2 is still necessary.

(6) Compliance with the requirements referred to in paragraph 5 is checked on a regular and random basis by an authorised official of the Federal Intelligence Service who is qualified to hold judicial office. If the check reveals that the data have been processed unlawfully, the data must be erased immediately under the supervision of an official of the Federal Intelligence Service who is qualified to hold judicial office. Paragraph 1 sentences 3 to 5 apply *mutatis mutandis*.'

3. In Section 7(1), 'Section 33 of the Federal Intelligence Service Act' is amended to 'Section 65(1) of the Federal Intelligence Service Act'.

4. Section 8 is amended as follows:

a) Paragraph 4 sentence 4 is worded as follows: 'Section 6(1), sentences 4 and 5, paragraph 2, sentences 1 and 2, and paragraphs 5 and 6, subject to the proviso that the further processing pursuant to paragraph 5, sentence 2, is only permitted for the purpose of identifying and responding to threats within the meaning of Section 8(1), shall apply *mutatis mutandis*.'
b) In paragraph 5, 'Section 33' is replaced by 'Section 65(1)'.

Article 3
Amendments to the Federal Civil Servants' Remuneration Act

[to be completed]

Article 4
Regulation on the technical and organisational implementation of measures for telecommunications surveillance (Telecommunications Surveillance Regulation, TKÜV)

Telecommunications Surveillance Regulation in the version promulgated on 11 July 2017 (*BGBl.* p. 2316), most recently amended by Article 27 of the Act of 20 November 2019 (*BGBl.* I p. 1724).

1. In Section 1(1)(e), the words 'Sections 6, 12 and 14 of the Federal Intelligence Service Act' are amended to 'Sections 19, 24 and 26 of the Federal Intelligence Service Act'.

2. In Section 1(4), the words 'Sections 6, 12 or 14 of the Federal Intelligence Service Act' are amended to 'Sections 19, 24 and 26 of the Federal Intelligence Service Act'.

3. In Section 2(1)(a), the words 'Section 9 of the Federal Intelligence Service Act' are amended to 'Section 25(1), sentence 1, of the Federal Intelligence Service Act'.

4. In Section 2(3)(a), the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

5. In Section 2(15), the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

6. In Section 2(17)(c), the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

7. In the heading of Part 3, the words ‘Sections 6, 12 and 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

8. In Section 27(1), sentence 1, the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act, the telecommunications that are transmitted through the telecommunications network referred to in the order, including the […] in this telecommunications network’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act, the telecommunications that are referred to in the order pursuant to Section 25(1), sentence 1, of the Federal Intelligence Service Act, including the […] in these telecommunications’.

9. In Section 27(8), sentence 2, the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act an order pursuant to Section 6(1), sentence 2, of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act an order pursuant to Section 25(1), sentence 1, of the Federal Intelligence Service Act’.

10. In Section 28(1), the words ‘Sections 6, 12 or 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

Article 5
Customs Administration Act (ZollVG)

Customs Administration Act of 21 December 1992 (*BGBl.* I p. 2125; 1993 I p. 2493), most recently amended by Article 210 of the Regulation of 19 June 2020 (*BGBl.* I p. 1328).

In Section 12a(8), the words ‘Section 8 of the Federal Intelligence Service Act’ are amended to ‘Section 10 of the Federal Intelligence Service Act’.

Article 6
Act on the prevention of threats to the security of the Federal Republic of Germany through the dissemination of high-quality remote sensing data (Satellite Data Security Act, SatDSiG)

Satellite Data Security Act of 23 November 2007 (*BGBl.* I p. 2590), most recently amended by Article 2 of the Act of 10 July 2020 (*BGBl.* I p. 1637).

In Section 27(1) sentence 2, the words ‘Section 23(3) of the Federal Intelligence Service Act’ are amended to ‘Section 10(3) of the Federal Intelligence Service Act’.

Article 7
Telecommunications Act (TKG)

Telecommunications Act of 22 June 2004 (*BGBl.* I p. 1190), most recently amended by Article 319 of the Regulation of 19 June 2020 (*BGBl.* I p. 1328).

1. In Section 110(1)(5), the words ‘Sections 6, 12 and 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

2. In Section 110(2), the words ‘Section 8(1), sentence 1, of the Federal Intelligence Service Act’ are amended to ‘Section 25(1), sentence 1, of the Federal Intelligence Service Act’.

3. In Section 114(1)(5), the words ‘Sections 6, 12 and 14 of the Federal Intelligence Service Act’ are amended to ‘Sections 19, 24 and 26 of the Federal Intelligence Service Act’.

Article 8
Act on the requirements and procedure for security clearances by the Federal Government and the protection of classified information (Security Clearances Act, SÜG)

Security Clearances Act of 20 April 1994 (*BGBl.* I p. 867), most recently amended by Article 20 of the Regulation of 19 June 2020 (*BGBl.* I p. 1328).

In Section 36(2), the words ‘Section 31 of the Federal Intelligence Service Act’ are amended to ‘Section 12 of the Federal Intelligence Service Act’, and the words ‘Section 21 of the Federal Intelligence Service Act’ are amended to ‘Section 18 of the Federal Intelligence Service Act’

Article 9
Act on the Central Register of Foreign Nationals (AZR Act)

AZR Act of 2 September 1994 (*BGBl.* I p. 2265), most recently amended by Article 167 of the Regulation of 19 June 2020 (*BGBl.* I p. 1328).

1. In Section 11(2), the words ‘Section 33 of the Federal Intelligence Service Act’ are amended to ‘Section 65(1) of the Federal Intelligence Service Act’.

2. In Section 34(3), the words ‘Section 22 of the Federal Intelligence Service Act’ are amended to ‘Section 9 of the Federal Intelligence Service Act’.

Article 10
Code of Criminal Procedure (StPO)

Code of Criminal Procedure in the version promulgated on 7 April 1987 (*BGBl.* I p. 1319), most recently amended by Article 2 of the Act of 9 October 2020 (*BGBl.* I p. 2075).

1. In Section 474(2), the words ‘Section 23 of the Federal Intelligence Service Act’ are amended to ‘Section 10 of the Federal Intelligence Service Act’.

2. In Section 492(4), the words ‘Section 23(3) of the Federal Intelligence Service Act’ are amended to ‘Section 10(3) of the Federal Intelligence Service Act’.

Article 11
Authorisation to publish a consolidated text

The Federal Chancellery is authorised to publish a consolidated text of the Federal Intelligence Service Act in the Federal Law Gazette in the version applicable as of the entry into force of this Act.

Article 12
Encroachment upon basic rights

Article 1(4) (Federal Intelligence Service Act) and Article 2 (G 10 Act) restrict the basic right to confidentiality of correspondence, post and telecommunications (Article 10 of the Basic Law).

Article 13
Entry into force

In Article 1(21), Sections 41, 43 to 50 and 53 of the Federal Intelligence Service Act will enter into force on the day after promulgation. This Act will otherwise enter into force on 1 January 2022. This Act will otherwise enter into force on 1 January 2022.