Headnotes

to the Judgment of the First Senate of 20 April 2016

– 1 BvR 966/09 — 1 BvR 1140/09 –

1. **a) The authorisation of the Federal Criminal Police Office to carry out covert surveillance measures (surveillance of private homes, remote searches of information technology systems, telecommunications surveillance, collection of telecommunications traffic data and surveillance outside of private homes using special means of data collection) is, for the purpose of protecting against threats from international terrorism, in principle compatible with the fundamental rights enshrined in the Basic Law.**

   b) The design of these powers must satisfy the principle of proportionality. Powers that constitute a serious interference with privacy must be limited to the protection or legal reinforcement of sufficiently weighty legal interests; require that a threat to these interests is sufficiently specifically foreseeable; may, only under limited conditions, also extend to third parties from whom the threat does not emanate and who belong to the target person's sphere; require, for the most part, particular rules for the protection of the core area of private life as well as the protection of persons subject to professional confidentiality; are subject to requirements of transparency, individual legal protection, and supervisory control; and must be supplemented by deletion requirements with regard to the recorded data.

2. **The requirements for the use and transfer of data collected by the state follow the principles of purpose limitation and change in purpose.**

   a) The scope of a purpose limitation depends on the specific legal basis for the data collection: the data collection initially takes its purpose from the respective investigation procedure.

   b) The legislature may allow a use of the data beyond the specific procedure of the data collection in the context of the original purposes of the data (further use). This implies that the use of collected data is limited to the same authority acting in the same function and for the protection of the same legal interests. For data from the surveillance of private homes or from access to information technology systems, each further use must additionally also fulfil the relevant risk situation requirements applicable to the data collection.

   c) Moreover, the legislature may also allow for a further use of data collected by the state for other purposes than those determining the original data collection (change in purpose).

   The proportionality requirements for such a change must conform to the principle of a hypothetical re-collection of data. According to this, the new use of the data must serve the protection of legal interests or aim to investigate criminal offences of such weight that would, by constitutional standards, justify collecting them again with comparably weighty means. A specific risk situation, as required for the initial data collection, is generally not required a second time; it is necessary but generally also sufficient that there be a specific evidentiary basis for further investigations.

   With regard to data from the surveillance of private homes and from remote searches of information technology systems, a change in purpose is only permitted if the relevant risk situation requirements applicable to the collection of the data are again fulfilled.

3. **The transfer of data to state authorities in third countries is subject to the general constitutional principles of purpose limitation and change in purpose. In assessing a new use, the autonomy of the other legal order must be respected. A transfer of data to third countries requires the ascertainment that, in the third country, the data will be handled in sufficient conformity with rule-of-law standards.**

FEDERAL CONSTITUTIONAL COURT

– 1 BvR 966/09 –

– 1 BvR 1140/09 –

Pronounced

on 20 April 2016

Sommer

Amtsinspektorin

as Registrar

of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaints

1. of Mr B…,
2. of Mr F…,
3. of Mr S…,
4. of Prof. Dr. H…,
5. of Dr. N…,
6. of Mr H…,

– authorised representatives: 1. Rechtsanwalt Dr. Dr. h.c. Burkhard Hirsch,
Rheinallee 120, 40545 Düsseldorf,

2. Rechtsanwalt Gerhart R. Baum,
Benrather Schloßallee 101, 40597 Düsseldorf –

against § 14, § 20c sec. 3, § 20g, § 20h, § 20k, § 20l, § 20u secs. 1 and 2, § 20v and § 20w of the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG) in the version of 31 December 2008 (Federal Law Gazette, *Bundesgesetzblatt* – BGBl 2008, pp. 3083 et seq.)

– 1 BvR 966/09 –,

1. of Mr W…,
2. of Mr S…,
3. of Dr. T…,

4. of Ms R…,
5. of Mr N…,
6. of Mr T…,
7. of Ms M…,
8. of Ms K…,
9. of Mr B…,

– authorised representative: Rechtsanwalt Sönke Hilbrans,
Immanuelkirchstraße 3-4, 10405 Berlin –

against a) § 20g secs. 1 and 2, § 20h secs. 1, 2 and 5,
§ 20j sec. 1, § 20k secs. 1 and 7,
§ 20l secs. 1 and 6, § 20m sec. 1,
§ 20v sec. 4 sentence 2 and sec. 6 sentence 5,
§ 20w sec. 2 sentences 1 and 2 BKAG,

b) § 20h sec. 5 sentence 10, § 20k sec. 7 sentence 8,
§ 20l sec. 6 sentence 10 BKAG,

c) § 20u secs. 1 and 2 BKAG in conjunction with
§ 53 sec. 1 sentence 1 nos. 2 and 3 of the Code of Criminal Procedure (*Strafprozessordnung* – StPO)

– 1 BvR 1140/09 –

the Federal Constitutional Court – First Senate –

with the participation of Justices

Vice-President Kirchhof,
Gaier,
Eichberger,
Schluckebier,
Masing,
Paulus,
Baer,
Britz

held on the basis of the oral hearing of 7 July 2015:

Judgment:

1. **§ 20h section 1 number 1 c of the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG) in the version of the Act on Prevention by the Federal Criminal Police Office of Threats from International Terrorism *(Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt)* of 25 December 2008 (Federal Law Gazette, *Bundesgesetzblatt* – BGBl I p. 3083) and in the version of later acts violates Article 13 section 1 of the Basic Law (*Grundgesetz* – GG) and is void.**

2. **§ 20v section 6 sentence 5 of the Federal Criminal Police Office Act violates Article 2 section 1 in conjunction with Article 1 section 1, Article 10 section 1, Article 13 section 1, each in conjunction with Article 19 section 4 of the Basic Law, and is void.**

3. **§ 14 section 1 (excluding sentence 1 number 2), § 20g sections 1 to 3, §§ 20h, 20j, 20k, 20l, § 20m sections 1 and 3, § 20u sections 1 and 2 and § 20v section 4 sentence 2, section 5 sentences 1 to 4 (excluding sentence 3 number 2), section 6 sentence 3 of the Federal Criminal Police Office Act are, according to the reasons of this decision, not compatible with Article 2 section 1 in conjunction with Article 1 section 1, Article 10 section 1, Article 13 sections 1 and 3 – also in conjunction with Article 1 section 1 and Article 19 section 4 of the Basic Law.**

4. **Until the Act is recast, however until 30 June 2018 at the latest, the provisions which have been declared incompatible with the Basic Law will stay in effect, subject to the condition that measures pursuant to § 20g section 2 numbers 1, 2 b, 4 and 5 of the Federal Criminal Police Office Act require a judicial order; in case of immediate danger, § 20g section 3 sentences 2 to 4 of the Federal Criminal Police Office Act applies correspondingly.**

   Measures pursuant to § 20g section 1 sentence 1 number 2, § 20l section 1 sentence 1 number 2 and § 20m section 1 number 2 Federal Criminal Police Office Act may only be ordered if the conditions set out in § 20k section 1 sentence 2 of the Federal Criminal Police Office Act, in the interpretation in conformity with the Basic Law as set out in the reasons of this decision, are fulfilled.

   The further use of data pursuant to § 20v section 4 sentence 2 of the Federal Criminal Police Office Act or the transfer of data pursuant to § 20v section 5 and § 14 section 1 of the Federal Criminal Police Office Act is permissible only in cases of imminent danger when data from the surveillance of private homes is concerned (§ 20h of the Federal Criminal Police Office Act); and only in cases of a specific impending danger to the relevant legal interests when data stemming from remote searches of information technology systems is concerned (§ 20k of the Federal Criminal Police Office Act).

5. **The constitutional complaint of complainant no. 4 in the proceedings 1 BvR 966/09 is rendered moot by his death.**

6. **For the rest, the constitutional complaints are rejected as unfounded.**

7. **The Federal Republic of Germany shall reimburse the complainants' necessary expenses incurred in the course of the constitutional complaint proceedings.**

R e a s o n s:

A.

I.

The constitutional complaints are directed against the provisions of the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG) inserted as Sub-Title 3a by the Act on Prevention by the Federal Criminal Police Office of Threats from International Terrorism of 25 December 2008 (Federal Law Gazette, *Bundesgesetzblatt* – BGBl I p. 3083), effective 1 January 2009. On the basis of Art. 73 sec. 1 no. 9a of the Basic Law (*Grundgesetz* – GG) (BGBl I p. 2034), created for this purpose in 2006, the federal legislature assigned the Federal Criminal Police Office tasks extending beyond its previous law enforcement duties, reaching into the domain of the protection against threats from international terrorism, a task hitherto 1

reserved solely for the *Laender* (federal states). An additional subject-matter of the constitutional complaints is the previously existing provision in the Federal Criminal Police Office Act on the transfer of data to third countries, the scope of which has been extended by the newly attributed powers.

II.

The constitutional complaints are directed, first, against the granting of various investigative powers. The challenged powers include the authorisation to question persons pursuant to § 20c BKAG, as well as the use of special means of data collection outside of private homes pursuant to § 20g secs. 1 to 3 BKAG including, in particular, the covert monitoring and recording of non-public speech, image recording, the application of tracking devices, and the use of police informants and undercover investigators. The constitutional complaints also challenge the power to carry out visual and acoustic surveillance of private homes pursuant to § 20h BKAG, to conduct electronic profile searching pursuant to § 20j BKAG, to access information technology systems pursuant to § 20k BKAG, to monitor on-going telecommunications pursuant to § 20l BKAG as well as to collect telecommunications traffic data pursuant to § 20m secs. 1 and 3 BKAG. Insofar, the challenges also encompass § 20u BKAG which deals with the protection of persons having the right to refuse to give evidence, as well as § 20w BKAG which sets out the duty to inform affected persons at the conclusion of the surveillance measure. 2

Second, the constitutional complaints are directed at provisions on the use of data. This affects, firstly, the provision on the use of data collected in accordance with Sub-Title 3a of the Act pursuant to § 20v sec. 4 sentence 2 BKAG by the Federal Criminal Police Office itself. The power pursuant to § 20v sec. 5 BKAG – with the exception of sentence 3 no. 2 – to transfer this data to other domestic public authorities is also challenged. Finally, § 14 sec. 1 sentence 1 nos. 1 and 3 and sentence 2, sec. 7 BKAG, which generally permits the transfer of data to authorities in third countries, is also challenged. § 14a BKAG, which additionally establishes a separate power to transfer personal data to Member States of the European Union, however, is not at issue in this proceedings. 3

[…] 4

III.

The complainants in the proceedings 1 BvR 966/09 are lawyers, journalists, a doctor and a certified psychologist, most of whom are active in the field of human rights politics. The complainants in the proceedings 1 BvR 1140/09 are former and current Members of the German *Bundestag* – acting here as private individuals –, who are also largely active in human rights politics and some of whom also work as lawyers or doctors. They claim a substantive violation of Art. 2 sec. 1 in conjunction with Art. 1 sec. 1, Art. 3 sec. 1, Art. 5 sec. 1 sentence 2, Art. 10, Art. 12, Art. 13, in part also in conjunction with Art. 1 sec. 1, Art. 19 sec. 4 GG and Art. 20 sec. 3 GG. 5

[…] 6-40

IV.

[…] 41-73

V.

[…] 74

B.

The constitutional complaints are for the most part admissible. 75

I.

The complainants' constitutional complaints are directed against the surveillance and investigative powers of the Federal Criminal Police Office, and thereby specifically also against the inadequate protection of the core area of private life as well as against the surveillance of persons having the right to refuse to give evidence, and against provisions on the use of data. The complaints are directed directly against the respective provisions authorising the Federal Criminal Police Office, but also indirectly against further provisions with which the legislature supplements these powers in order to guarantee their proportionality and without which their constitutionality cannot be evaluated. Upon a reasonable interpretation of the constitutional complaints, the challenges thus cover § 14 sec. 1 sentence 1 nos. 1 and 3, sentence 2, sec. 7, § 20c, § 20g secs. 1 to 3, § 20h, § 20j, § 20k, § 20l, § 20m secs. 1 and 3, § 20u secs. 1, 2 and 4, § 20v sec. 4 sentence 2, sec. 5 (except sentence 3 no. 2 regarding which the complaint was not substantiated) and sec. 6 as well as § 20w BKAG. 76

II.

[…] 77-78

III.

The constitutional complaints are admissible for the rest. 79

1. The complainants have standing to lodge a constitutional complaint. They claim that the challenged provisions may be directly violating their fundamental rights. […] 80

2. The challenged provisions affect the complainants directly, individually and presently. Their constitutional complaints thus fulfil the specific requirements for constitutional complaints lodged directly against a statute. 81

a) The complainants do not lack the condition of being directly affected. Admittedly, the challenged powers must be implemented by means of further executing acts. However, a statute is also deemed to directly affect complainants in cases where they cannot pursue a legal remedy due to the fact that they do not actually gain knowledge of any action being executed. In such cases, they have standing to lodge a constitutional complaint directly against a statute (cf. Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 133, 277 <311 para. 83>; established case-law). In principle, the investigative and surveillance measures authorised by the challenged provisions are carried out covertly. The obligations to notify contained in the Act only partially compensate for this, since they possibly take effect much later in time and provide for broad exceptions. The parties concerned will, in general, not be informed of the further use or transfer of the data allowed by the challenged provisions either. The complainants should therefore not be made to await the execution of the relevant actions in order to challenge these. 82

b) The complainants are also affected individually and presently. 83

The complainants submit that due to their specific political, professional and private connections to potential persons targeted by the challenged measures there is sufficient probability of them being affected. They submit that by reason of their political activity, their professional activity as lawyers or psychotherapists, or their commitment to matters of human rights, they may easily come into contact with persons whom a link with international terrorism may be imputed to. Given the broad scope of the challenged provisions, which are not tailored to a specific limited group of persons but rather, pursuant to § 4a BKAG, serve to prevent international terrorism generally and thus can also broadly affect third parties acting in good faith, it is demonstrated that there is sufficient probability that their own rights are presently affected (cf. BVerfGE 109, 279 <307 and 308>; 113, 348 <363 and 364>; 133, 277 <312 et seq. paras. 86 and 87>). 84

3. […] 85

C.

Insofar as the constitutional complaints are directed against the investigative and surveillance powers, they are well-founded in several respects. 86

I.

In respect of legislative competences, meanwhile, the challenged provisions are constitutional. 87

[…] 88-89

II.

The challenged surveillance and investigative powers authorise interferences with fundamental rights, which, depending on which fundamental right is affected and on the varying weight of the interference, must individually be measured against the principle of proportionality and the principle of legal clarity and specificity. The powers have in common that the potential interferences they authorise are for the most part very serious, yet since their objective is to protect against the threat of international terrorism, they have a legitimate aim and are, to that end, suitable and necessary. 90

1. The challenged powers authorise the Federal Criminal Police Office to covertly collect personal data in the context of the protection against threats and the prevention of criminal offences. This allows for – depending on the power in question – interferences with the fundamental rights of Art. 13 sec. 1, Art. 10 sec. 1 and Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG, the latter both in its manifestation as the right to the guarantee of the confidentiality and integrity of information technology systems as well as the right to informational self-determination. 91

All these powers provide the legal bases for investigative and surveillance measures which are usually carried out covertly without the knowledge of the parties concerned and can constitute a serious interference with privacy. Even if legitimate expectations of confidentiality are affected to differing degrees and the powers' weight of interference varies significantly, these powers generally all have a weight of interference which weighs heavily in any case. Only individual measures pursuant to § 20g secs. 1 and 2 BKAG constitute an exception. 92

2. The constitutionality of the powers depends on the limits arising from each of these fundamental rights and the proportionality requirements which must be determined for each of the powers. According to the principle of proportionality, the granting of these powers must always pursue a legitimate aim and must be suitable, necessary and, in the strict sense, proportionate to achieving this aim (cf. BVerfGE 67, 157 <173>; 70, 278 <286>; 104, 337 <347 et seq.>; 120, 274 <318 and 319>; 125, 260 <316>; established case-law). 93

Furthermore, the challenged powers are to be measured against the principle of legal clarity and specificity, which aims to increase the predictability of interferences for citizens, constitute an effective limit to administrative powers and enable effective judicial review (cf. BVerfGE 113, 348 <375 et seq.>; 120, 378 <407 and 408>; 133, 277 <336 para. 140>; established case-law). With regard to the powers in question here that pertain to the covert collection and processing of data, and that have the potential to constitute serious interferences with privacy, the principle sets up particularly strict requirements. Since affected persons can for the most part neither notice nor challenge the use of these powers, their content – in contrast to, for example, administrative law terms that are open to interpretation and executed by means of an administrative act – can only be rendered more specific to a very limited extent within the interplay between actual application and judicial review. Individually, however, the requirements differ, depending on the weight of the interference, and are thus tightly linked to the respective substantive requirements of proportionality (cf. BVerfGE 110, 33 <55>; 113, 348 <376>). 94

3. The challenged provisions pursue a legitimate aim and are suitable and necessary to that end. 95

a) The powers pursue a legitimate aim. They provide the Federal Criminal Police Office with means of gathering information which it can use in fulfilling its new task of protecting against threats from international terrorism. The term “international terrorism” as set out in the description of tasks in § 4a sec. 1 BKAG and its reference to § 129a secs. 1 and 2 of the Criminal Code (*Strafgesetzbuch* – StGB) is, in line with the EU Framework Decision of 13 June 2002 and international terminology (OJ L 164, p. 3; Draft Comprehensive Convention on International Terrorism, in: Measures to eliminate international terrorism, Report of the Working Group of 3 November 2010, UN Doc. A/C.6/65/L.10) and – in conformity with the notions of the constitution-amending legislature upon the creation of Art. 73 sec. 1 no. 9a GG (cf. *Bundestag* document, *Bundestagsdrucksache* – BTDrucks 16/813, p. 12), limited to specifically characterised criminal offences of particular weight. Criminal offences characterised as terrorism in this sense aim to destabilise society and comprise, in a reckless instrumentalisation of other people, attacks on the life and limb of random third parties. They are directed against the basic pillars of the constitutional order and of society as a whole. The provision of effective means of gathering information for protecting against terrorism constitutes a legitimate aim and is of great significance for a democratic and free basic order (cf. BVerfGE 115, 320 <357 and 358>; 120, 274 <319>; 133, 277 <333 and 334 para. 133>). 96

b) The granting of the surveillance and investigative powers in question is suitable for achieving this aim. They provide the Federal Criminal Police Office with the means for gathering information that can play a role in countering the threat of international terrorism. The different powers are, at least in principle, necessary for this. Each power allows specific measures that cannot always be replaced by others. Less intrusive measures that provide equally effective and broad possibilities for gathering information for protecting against international terrorism are not apparent. Evidently, this does not affect the fact that in each individual case, the exercise of these powers, too, must be in accordance with the concepts of suitability and necessity. 97

III.

Limitations result mainly from the requirements of proportionality in the strict sense. Accordingly, the surveillance and investigative powers must be appropriately designed with a view to the weight of the interference. It is the legislature’s task to balance the seriousness of the interferences with fundamental rights of the potentially affected persons that are at issue here, on the one hand, with the duty of the state to protect the fundamental rights of its citizens, on the other. 98

1. The legislature must thereby take into account, on the one hand, the weight of the interference of the measures allowed by the challenged provisions. These allow – to differing degrees, depending on the power – far-reaching interferences with privacy and can, in individual cases, even intrude upon private refuges the protection of which is of particular significance for the safeguarding of human dignity. The legislature must also consider the developments of information technology which increasingly extend the scope of surveillance measures, facilitate their operability, and enable making connections, which can go so far as to create personality profiles. In each case, differentiations must be based on the respective power in question as well as the fundamental rights it affects. 99

2. On the other hand, the legislature must ensure the effective protection of the fundamental rights and legal interests of citizens. With regard to the constitutional appropriateness test, it must be taken into account that the constitutional order, the existence and the security of the Federation and of the *Laender* (federal states), and life, limb and the freedom of persons are legally protected interests of significant constitutional weight. Accordingly, the Federal Constitutional Court has underlined that the security of the state, as a constituted power of peace and order, as well as the safety of the population it is bound to guarantee – while respecting the dignity and the intrinsic value of the individual – rank equally with other highly valued constitutional rights. It thus considers the state to be under an obligation to protect the life, physical integrity and freedom of the individual, which also means, in particular, to protect against unlawful interferences by others (cf. BVerfGE 115, 320 <346 and 347>; see also BVerfGE 49, 24 <56 and 57>; 90, 145 <195>; 115, 118 <152 and 153>). 100

In testing appropriateness, it must also be considered that the challenged provisions do not constitute provisions whose broad scope of interference affect the entire population equally. Rather, these are predominantly provisions aimed at enabling security authorities to protect, in individual cases, legal interests having constitutional rank from serious threats as well as to prevent criminal offences of great weight. 101

In light of the threat posed by international terrorism, the decision to collect data is also of particular significance for the exchange of information between domestic authorities as well as for rendering the cooperation with security authorities of other states as effective as possible. A functioning exchange of information, which is in the interest of the constitutionally required protection of persons, presupposes the transfer of information gathered domestically and in return relies on information from third countries. 102

IV.

For powers of investigation and surveillance constituting serious interferences with privacy, which are predominantly in question here, the Federal Constitutional Court has derived overarching requirements from the principle of proportionality in the strict sense. These concern specific wide-ranging potential threats to fundamental rights, in particular those entailed in the context of electronic processing of data (cf. BVerfGE 100, 313 <358 et seq.>; 115, 320 <341 et seq.>; 125, 260 <316 et seq.>; 133, 277 <335 et seq. para. 138 et seq.>), as well as individual case-by-case measures against persons who are being focussed on by the acting authorities (BVerfGE 107, 299 < 312 et seq.> - Collection of telecommunications traffic data -, BVerfGE 110, 33 <52 et seq.>; 113, 348 <364 et seq.>; 129, 208 <236 et seq.> - Telecommunications surveillance under federal, federal state and criminal procedural law -, BVerfGE 109, 279 <335 et seq.> - Surveillance of private homes -, BVerfGE 112, 304 <315 et seq.> - GPS observation -, BVerfGE 120, 274 <302 et seq.> - Online search -). 103

1. Covert surveillance measures, to the extent that they seriously interfere with privacy, as most of the measures at issue here do, are only compatible with the Constitution if they pursue the aim of protecting or legally reinforcing sufficiently weighty legal interests when these are in danger or are violated, as evidenced by strong factual indications in the specific case. They generally require that the person targeted by the measure would be considered, by a reasonable person examining the objective circumstances, to be involved in a potential violation of a legal interest. A mere possibility based primarily on the intuition of the security authorities that further intelligence might be obtained is not sufficient for carrying out such measures (see BVerfGE 107, 299 <321 et seq.>; 110, 33 <56>; 113, 348 <377 and 378, 380 and 381>; 120, 274 <328>; 125, 260 <330>). The Constitution thus sets clear limits to lowering the threshold for crime prevention measures that are carried out covertly and can seriously interfere with privacy; in contrast, with regard to measures involving less serious interferences with privacy, the constitutionally permitted leeway in crime prevention matters is broader. 104

With regard to the detailed design of the individual powers, what matters substantially for their appropriateness as well as the required specificity is that they be tailored to the weight of each codified interference. The more seriously the surveillance measures interfere with privacy and thwart legitimate expectations of confidentiality, the stricter the requirements must be. The surveillance of private homes and the access to information technology systems constitute particularly serious interferences with privacy. 105

a) Covert surveillance measures must be limited to the protection or legal reinforcement of sufficiently weighty legal interests. 106

For measures that serve a law enforcement purpose and are thus repressive in nature, the weight of the criminal offences in question is relevant for their classification, which the legislature has divided into significant, serious and particularly serious– criminal offences, each defined in greater detail. Thus, the surveillance of private homes requires the suspicion of a particularly serious criminal offence (cf. BVerfGE 109, 279 <343 et seq.>); telecommunications surveillance or the use of telecommunications traffic data collected as a precaution requires the suspicion of a serious criminal offence (cf. BVerfGE 125, 260 107

<328 and 329>; 129, 208 <243>); while the collection of telecommunications traffic data with cause or observation by means of a GPS tracker, for example, requires a significant criminal offence – and, in the former case, one that is specified in the law – (cf. BVerfGE 107, 299 <321 and 322>; 112, 304 <315 and 316>; with regard to the latter decision, see also European Court of Human Rights (ECtHR), Uzun v. Germany, judgment of 2 September 2010, no. 35623/05, para. 70, Neue Juristische Wochenschrift – NJW 2011, p. 1333 <1336>, on Art. 8 of the European Convention on Human Rights – ECHR).

With regard to measures that serve to protect against threats and are thus of a preventive nature, what matters is the weight of the legal interests being protected (cf. BVerfGE 125, 260 <329>). Covert surveillance measures that constitute a serious interference with privacy are only permissible with regard to particularly weighty legal interests. These include life, limb and the freedom of persons as well as the existence or security of the Federation or a *Land* (cf. BVerfGE 120, 274 <328>; 125, 260 <330>) In contrast, the Federal Constitutional Court has not deemed the unlimited protection of proprietary interests to be sufficiently weighty. However, the Court has held that access to data stored as a precaution (cf. BVerfGE 125, 260 <330>) or the surveillance of private homes also in cases of general danger (cf. BVerfGE 109, 279 <379>), or remote searches of information technology systems [translator's note: previous translations of the German term *Onlinedurchsuchung* have used "online search"; this translation uses "remote search" with the same meaning] in cases of danger to interests of the public that affect the existence of people (cf. BVerfGE 120, 274 <328>) are generally compatible with the Constitution. Against that background, the legislature is not hindered from uniformly establishing the relevant threshold for the protection of legal interests with regard to these surveillance measures. 108

b) In the context of the protection against threats to the legal interests mentioned above, the collection of data by means of covert surveillance measures having a high interference intensity is generally only proportionate if there is a sufficiently specific foreseeable danger to these legal interests in an individual case and the person targeted by these measures appears, to a reasonable person examining the objective circumstances, to be involved therein (cf. BVerfGE 120, 274 <328 and 329>; 125, 260 <330 and 331>). 109

These conditions also depend, in each case, on the type and weight of the interference. For the particularly serious interferences with privacy that the surveillance of private homes constitutes, Art. 13 sec. 4 GG requires imminent danger. The term "imminent danger" thereby not only refers, in the sense of the qualified protection of legal interests, to the extent, but also to the probability, of damage (cf. BVerfGE 130, 1 <32>). 110

Furthermore, the requirements of a sufficiently specific foreseeable risk situation with respect to the mentioned legal interests must be determined in relation to the burden on the affected person. Sufficient from a constitutional perspective are the requirements for the prevention of specific, directly imminent or present threats from persons subject to police action (*polizeipflichtige Personen*) according to the standards of general security law pertaining to the legally protected interests relevant here. The traditional police law term "specific threat" requires a factual situation that in the specific case, if left unhindered and provided that the events proceed in line with what is objectively to be expected, will lead, in foreseeable time, and with sufficient probability, to a violation of an interest protected by the police (cf. BVerfGE 115, 320 <364>; Decisions of the Federal Administrative Court, *Entscheidungen des Bundesverwaltungsgerichts* – BVerwGE 116, 347 <351>). An even closer temporal link is required when the respective legal authorisation requires a "directly imminent" or "present threat" (cf. BVerwGE 45, 51 <57 and 58>). 111

However, the legislature is not constitutionally limited at the outset to creating, in respect of each type of function, criteria for interferences that reflect the usual model in security law of protecting against specific, directly imminent or present threats. Rather, it can set wider limits for particular fields, in order to aim at already preventing criminal offences, by lowering the requirements of foreseeability of the causal chain. However, the legal basis for the interference must then also require a sufficiently specified threat, in the sense that there be at least factual indications of the emergence of a specific threat to the legally protected 112

interests. General experience alone is not sufficient for justifying an interference. Rather, certain facts must be determined that, in the individual case, substantiate the prognosis that an event leading to an imputable violation of the legally protected interests relevant here will occur (cf. BVerfGE 110, 33 <56 and 57, 61>; 113, 348 <377 and 378>). A sufficiently specific threat in this sense may already exist even where the causal chain leading to the damage is not yet foreseeable with sufficient probability, as long as certain facts already indicate that a threat to an exceptionally significant legal interest may occur. In such a case, the facts must allow the inference of, firstly, an occurrence that can be specified at least with regard to its type and which is temporally foreseeable, and, secondly, of the involvement of persons whose identity has at least been determined to the extent that the surveillance measure can target them specifically and is largely limited to them (BVerfGE 120, 274 <328 and 329>; 125, 260 <330 and 331>). With regard to terrorist offences, which are often committed at unforeseeable locations, planned far in advance by individuals who have no criminal record, and carried out in very different ways, surveillance measures may also be authorised if, despite the lack of a temporally foreseeable occurrence of a specific type, the individual behaviour of a person substantiates the specific probability that the person will commit such offences in the near future. For instance, this is conceivable in the case of a person entering the Federal Republic of Germany after having been abroad at a training camp for terrorists.

In contrast, the weight of interference of covert police surveillance measures is not sufficiently taken into account when the factual grounds for the interference are shifted so as to include the preliminary stages of a still vague and unforeseeable specific threat to the legal interests protected by the provision. Linking the threshold for interference to the preliminary stages is constitutionally unacceptable if there are only relatively diffuse indications for potential threats, given the weight of the interference. The factual situation at such a stage is often characterised by the rather ambivalent meaning of individual observations. While occurrences may remain harmless, they might also be part of a process that develops into a threat (cf. BVerfGE 120, 274 <329>; see also BVerfGE 110, 33 <59>; 113, 348 <377>). Such openness is not sufficient as a basis for carrying out covert and highly intrusive surveillance measures. For example, the mere knowledge that a person is attracted to a fundamentalist understanding of religion would not be sufficient for such measures. 113

c) Tiered requirements arise with regard to the extent to which surveillance measures can be carried out in a target person's sphere where the measures also affect persons not responsible for particular actions or circumstances or who are not suspects and therefore bear no special responsibility. 114

Access to information technology systems and the surveillance of private homes may only directly target persons responsible for impending or imminent dangers (cf. BVerfGE 109, 279 <351, 352>; 120, 274 <329, 334>). These measures constitute such a serious interference with privacy that they cannot be extended to other persons. It is not constitutionally objectionable for measures targeting the persons responsible to also cover third parties, so long as this is inevitable (cf. BVerfGE 109, 279 <352 et seq.>). Thus, the surveillance of the home of a third party may be authorised, if on the basis of certain facts it can be supposed that the target person will be present while the measure is carried out, will conduct conversations relevant to the investigation there, and the surveillance of that person's own home would not in itself be sufficient for investigating the factual circumstances (cf. BVerfGE 109, 279 <353, 355 and 356>). Likewise, a remote search may be extended to the information technology systems of third parties if factual indications suggest that the target person has saved information relevant to the investigation there and access solely to the target person's own information technology system would not be sufficient for achieving the aims of the investigation. 115

The ordering of other covert surveillance measures directly targeting third parties is not impermissible *per se* . It is conceivable that the surveillance of persons – to be clearly defined – in the target person's sphere be authorised, for instance with regard to contacts or messengers. The justification for such authorisation lies in the objective nature of protecting against threats and of truth-finding in criminal investigations. The extension of such an authorisation to third parties is subject to strict proportionality requirements and requires a specific individual proximity of the person concerned to the threat or criminal 116

offence being investigated. In that respect it is not sufficient that there merely be some sort of contact with the target person. Rather, further indications are needed showing that the contact is relevant to the object of the investigation and that there is thus a non-negligible probability that the surveillance measure will contribute to elucidating the threat (cf. BVerfGE 107, 299 <322 and 323>; 113, 348 <380 ad 381>). The surveillance of persons that – based merely on the fact that they have been in contact with the target person – attempts to find out whether this can result in further evidentiary bases for further investigations, is constitutionally impermissible. With regard to these contact persons, however, the Constitution does not bar investigative measures that entail a lower level of interference from aiming to thereby attain the threshold for surveillance measures entailing a higher level of interference.

2. Overarching procedural requirements also derive from the principle of proportionality. The investigative and surveillance measures in question here, which predominantly involve serious interferences, and regarding which it can be presumed that they will also record highly private information, and that are carried out covertly without the knowledge of the affected persons, as a rule require prior review by an independent body, in the form, for example, of a judicial order (on this, see also ECtHR, Klass and others v. Germany, judgment of 6 September 1978, no. 5029/71, para. 56; ECtHR (Grand Chamber), Zakharov v. Russia, judgment of 4 December 2015, no. 47143/06, paras. 258, 275; ECtHR, Szabó and Vissy v. Hungary, judgment of 12 January 2016, no. 37138/14, para. 77). For measures relating to the surveillance of private homes this already results from Art. 13 secs. 3 and 4 GG (cf. in this respect BVerfGE 109, 279 <357 et seq.>) and directly follows from the principle of proportionality (cf. BVerfGE 120, 274 <331 et seq.>; 125, 260 <337 et seq.>). 117

The legislature must combine the imperative of a precautionary independent review framed in specific and legally clear form with strict requirements in respect of the content and the reasons for judicial orders. Also deriving from this is the requirement that the application for an order have a sufficiently substantiated justification and limits, which makes it possible in the first place for the courts or an independent body to exercise effective review. In particular, the authority submitting the application must provide comprehensive information on the situation in question (cf. BVerfGE 103, 142 <152 and 153>). In connection with this, it is the duty and obligation of the court or the other decision-makers to independently reach a decision on whether the covert surveillance measure being applied for fulfils the legal requirements. The needed material and staffing requirements must be provided by the judicial administration of the *Laender* and the Chief Justice of the competent court (cf. BVerfGE 125, 260 <338>). 118

3. In addition to the constitutional requirements for the general conditions for interference, the respective fundamental rights in conjunction with Art. 1 sec. 1 GG give rise to particular requirements with regard to the protection of the core area of private life in the context of surveillance measures causing a particularly serious interference. 119

a) The constitutional protection of the core area of private life guarantees a highly private area for the individual which is free from surveillance. It has its roots in each of the fundamental rights affected by surveillance measures in conjunction with Art. 1. sec. 1 GG and ensures a core of human dignity that is beyond the state's reach and provides constitutional protection against such measures. Even paramount interests of the general public cannot justify an interference with this absolutely protected area of private life (cf. BVerfGE 109, 279 <313>; established case-law). 120

The possibility of expressing inner processes such as impressions and feelings, as well as reflections, views, and experiences of a highly personal nature belongs to the free development of personality in the core area of private life (cf. BVerfGE 109, 279 <313>; 120, 274 <335>; established case-law). Particular protection is afforded to non-public communication with persons enjoying the highest level of personal trust, conducted under the reasonable assumption that no surveillance is taking place, as is the case, in particular, in a private home. This group of persons includes, in particular, spouses or partners, siblings and direct relatives in ascending or descending line, in particular if they live in the same household, and can also include defence counsel, doctors, the clergy and close personal friends (cf. BVerfGE 109, 279 121

<321 et seq.>). This group only partially overlaps with those persons who have the right to refuse to give evidence. These conversations do no lose their overall highly personal character merely because they combine highly personal with everyday matters (cf. BVerfGE 109, 279 <330>; 113, 348 <391 and 392>).

In contrast, communication directly about criminal offences is not protected, not even when it also covers highly personal elements. The discussion and planning of criminal offences is not content that belongs to the core area of private life, but rather is of societal relevance (cf. BVerfGE 80, 367 <375>; 109, 279 <319 and 302, 328>; 113, 348 <391>). Of course this does not mean that the core area is subject to a general balancing requirement with regard to public safety interests. A highly personal conversation does not fall outside the core area of private life simply because it could provide helpful insights for the investigation of criminal offences or dangers. Recordings or statements made in the course of a dialogue that only reveal, for instance, inner impressions and feelings and do not contain any indications with regard to specific criminal offences, do not simply become relevant to society by the fact that they might elucidate the reasons or motives for criminal behaviour (cf. BVerfGE 109, 279 <319>). Furthermore, despite having some link to criminal offences, situations in which individuals are in fact encouraged to admit wrongdoing or to prepare for the consequences thereof, such as confessions or confidential conversations with a psychotherapist or defence counsel, belong to the core area of private life, from which the state is absolutely excluded (cf. BVerfGE 109, 279 <322>). There is sufficient societal relevance, however, when the subject of conversations – even with highly trusted persons – is directly focused on criminal offences (cf. BVerfGE 109, 279 <319>). 122

b) Any surveillance measure must take into consideration the core area of private life. If it typically leads to the collection of data relevant to the core area, the legislature must provide provisions that guarantee effective protection in a legally clear manner (cf. BVerfGE 109, 279 <318 and 319>; 113, 348 <390 and 391>; 120, 274 <335 et seq.>). Powers that do not tend to lead to interferences do not require such provisions. Limits that in individual cases might arise here with regard to access to highly personal information must be applied directly, on constitutional grounds. 123

c) The protection of the core area of private life is strict and cannot be relativized through a weighing with security interests in accordance with the principle of proportionality (cf. BVerfGE 109, 279 <314>; 120, 274 <339>; established case-law). This does not mean that every instance in which highly personal information is indeed collected constitutes a violation of the Constitution or of human dignity. Given the uncertainty of action and prognosis under which security authorities carry out their duties, an unintentional intrusion upon the core area of private life in the course of a surveillance measure cannot be excluded ahead of time in every case (cf. BVerfGE 120, 274 <337 and 338>). However, the Constitution does require that in the design of surveillance measures, the respect of the core area be drawn as a strict limit, insurmountable by considerations in individual cases. 124

aa) Thus, firstly, it is absolutely impermissible to make the core area a target of state investigations and use information from these in any way or to otherwise use it as a basis for further investigations. Even if additional findings could result from it, a targeted interference with core privacy – not including the discussion of criminal offences (see above, C IV 3 a) – is ruled out from the outset. The protection of the core area cannot be subject to the proviso that interests must be balanced in individual cases. 125

bb) Furthermore, it also follows that, when carrying out surveillance measures, the protection of the core area must be taken into account on two levels. Firstly, at the data collection level, arrangements must be made in order to rule out as far as possible the unintentional collection of information stemming from the core area. Secondly, at the level of the subsequent analysis and use of the information, the consequences of an intrusion into the core area of private life that was not prevented must be strictly minimised (see BVerfGE 120, 274 <337 et seq..>; 129, 208 <245 and 246>). 126

d) In this context, the legislature must design the protection of the core area of private life differently for each surveillance measure, depending on the type of power and its proximity to the absolutely protected area of private life (cf. BVerfGE 120, 274 <337>; 129, 208 <245>). In doing so, it must, however, make 127

legislative arrangements on both levels.

At the data collection level, with regard to measures likely to result in interference, a pre-emptive examination must ensure that situations or conversations relevant to the core area are excluded to the extent that this can be done in advance, practicably and with a reasonable amount of effort (cf. BVerfGE 109, 279 <318, 320, 324>; 113, 348 <391 and 392>; 120, 274 <338>). Under certain circumstances, with regard to conversations with persons enjoying the highest level of personal trust, which are typically indicative of confidential situations, the presumption may be warranted that these belong to the core area and may not be subject to surveillance (cf. BVerfGE 109, 279 <321 et seq.>; 129, 208 <247>). The legislature may design this presumption to be refutable and in particular make it dependent on whether there are indications in an individual case that criminal acts will be discussed. In contrast, the fact that apart from highly personal issues, everyday matters will also be discussed is not sufficient to refute the highly confidential nature of a conversation (cf. BVerfGE 109, 279 <330 >). In any case, the measure must be discontinued when it becomes apparent that the surveillance is intruding upon the core area of private life (cf. BVerfGE 109, 279 <318, 324, 331>; 113, 348 <392>; 120, 274 <338>). 128

At the level of analysis and use of data, the legislature must provide for cases in which it was not possible to avoid collecting information relevant to the core area, by requiring, as a rule, the screening of the collected data by an independent body that filters out the information relevant to the core area prior to use by the security authorities (cf. BVerfGE 109, 279 <331 et seq.>; 120, 274 <338 and 339>). However, the constitutionally required procedural safeguards do not, in every type of case, require the creation of independent bodies other than the investigative bodies of the state (cf. BVerfGE 129, 208 <250>). The necessity of such a screening depends on the type, as well as, if applicable, the design of the power in question. The more reliably the collection of information relevant to the core area is already avoided at the first level, the more likely a screening by an independent body can be dispensed with, and vice versa. This does not affect the fact that the legislature has the possibility to enact the necessary provisions to provide the investigative bodies of the state with short-term possibilities for action in exceptional cases in case of immediate danger. In any case, the legislature must provide for the immediate deletion of any highly personal data collected and ensure that it be cannot be used at all. The deletion is to be documented in a manner that renders a subsequent review possible (cf. BVerfGE 109, 279 <318 and 319, 332 and 333>; 113, 348 <392>; 120, 274 <337, 339>). 129

4. Separate constitutional limits arise with regard to interplay between the different surveillance measures. Surveillance taking place over an extended period of time, encompassing almost every movement and expression of the person under surveillance and that could constitute the basis for a personality profile, is incompatible with human dignity (cf. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; established case-law). With the use of modern and in particular covert investigative methods, security authorities must, with respect to the potential for harm inherent in the “additive” interference with fundamental rights, coordinate to ensure that the overall extent of surveillance remains limited (cf. BVerfGE 112, 304 <319 and 320>). The limits on an exchange of data between authorities arising from the principle of purpose limitation (*Zweckbindung*) remain unaffected by this (see below, D I). 130

5. Out of proportionality considerations, separate constitutional limits to covert surveillance measures may arise with regard to certain groups of professionals or other persons, whose activities are constitutionally deemed to be particularly confidential. The legislature must ensure that the authorities respect these limits when ordering and carrying out surveillance measures. 131

As a rule, the legislature is not required to completely exempt certain groups of persons from surveillance measures in advance (cf. BVerfGE 129, 208 <262 et seq.>), given the already very high requirements for ordering such measures and the great significance of an effective protection against terrorist threats for the free and democratic order (cf. BVerfGE 115, 320 <357 and 358>; 120, 274 <319>; 133, 277 <333 and 334 para. 133>) and for the safety of persons, as well as with a view to the multitude of 132

considerations to be balanced, and, at the same time, with a view to the necessity of limiting opportunities for misuse. Rather, it may generally predicate the protection of confidentiality upon a weighing of considerations in the individual case.

The legislature has leeway to design with regard to establishing and delimiting the confidential relationships that are to be protected. It must balance the public's interest in the effective protection against threats with the weight of the measures for persons subject to professional confidentiality who depend upon a particular degree of confidentiality. In doing so, it must not only take into account the specific weight of the interference that such a measure constitutes for these persons with regard to their generally relevant fundamental rights, but also consider its effects on other fundamental rights, particularly Art. 4 sec. 1, Art. 5 sec. 1 and Art. 12 sec. 1 GG, or the independent mandate pursuant to Art. 38 sec. 1 GG. Insofar as it subjects certain professional groups to a stricter protection, these groups must be suitably delimited from the surveillance targets. 133

6. The principle of proportionality also sets requirements for transparency, the judicial protection of individuals, and supervisory control (BVerfGE 133, 277 <365 para. 204>; see also BVerfGE 65, 1 <44 et seq.>; 100, 313 <361, 364>; 109, 279 <363 and 364>; 125, 260 <334 et seq.>; established case-law; cf. similarly the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data of 25 January 2012, COM/2012/010 final – as of the conclusion of the trilogue, 16 December 2015: 15174/15; as of 28 January 2016: 5463/16, annex). The requirements applicable in this respect are derived from the fundamental right in question in conjunction with Art. 19 sec. 4 GG (cf. BVerfGE 125, 260 <335>; 133, 277 <366 para. 206>). 134

The transparency of data collection and processing should contribute to the emergence of trust and legal certainty as well as to the on-going addressing of the topic of data handling within a democratic discourse (BVerfGE 133, 277 <366 para. 206>). Its aim is to provide, as far as possible, subjective legal protection to affected parties, while at the same time counteracting the diffuse sense of threat emerging from covert state surveillance (cf. BVerfGE 125, 260 <335>; similarly Court of Justice of the European Union – ECJ, Digital Rights Ireland Decision, C-293/12, EU:C:2014:238, para. 37). The less it is possible to ensure subjective legal protection, the greater the significance of effective supervisory control and of transparency in the actions of the authorities vis-à-vis the public (cf. BVerfGE 133, 277 <366 and 367 para. 207>). 135

a) Another requirement for the proportionate design of the surveillance measures in question is a legislative provision ordering an obligation to notify. Given that such measures must be carried out covertly in order to achieve their aim, the legislature, in order to ensure subjective legal protection within the meaning of Art. 19 sec. 4 GG, must ensure that the affected persons are generally notified, at least subsequently, of the surveillance measures. The legislature may provide for exceptions by weighing the notification against the constitutionally protected legal interests of third parties. These must, however, be restricted to what is absolutely necessary (BVerfGE 125, 260 <336>). […] If there are compelling reasons for ruling out a subsequent notification, this must be confirmed by a judge and reviewed at regular intervals (BVerfGE 125, 260 <336 and 337>). 136

b) As a supplement to information-related interferences the carrying out or scope of which the affected persons cannot assess with certainty, the legislature must provide information rights. Restrictions are only permissible if they serve opposing interests of even greater weight. Legislative exclusionary criteria must ensure that the affected interests are comprehensively weighed against one another, taking into account the individual case in question (BVerfGE 120, 351 <365>). Should the practical effectiveness of such rights to information nevertheless remain limited, given the type of tasks being performed – as for example in the case of covert data processing for the protection against threats from international terrorism –, this is constitutionally acceptable (cf. BVerfGE 133, 277 <367 and 368 paras. 209 et seq.>). 137

c) In light of Art. 19 sec. 4 GG, a proportionate design of surveillance measures further requires that following notification, the affected persons may obtain, in a reasonable manner, judicial review of legality (in this respect see also Arts. 51 and 52 of the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, loc. cit.). 138

Moreover, proportionate design requires effective sanctions for violations of rights. If serious violations of the conditions for interference were to ultimately remain without sanction, resulting in atrophy of the protection of the right to personality due to its intangible nature, this would be contradictory to the duty of the state to effectively protect the development of personality. This could in particular be the case if the unauthorised collection or use of data were to routinely remain without any counterbalancing satisfaction or compensation for the affected person, due to lack of material damage. In this regard, however, the legislature has wide legislative discretion (cf. BVerfGE 125, 260 <339 and 340>, with further references). 139

d) Since with regard to covert surveillance measures, the transparency of data collection and data processing as well as the facilitation of the protection of the rights of individuals can be ensured only to a very limited degree, the guarantee of effective supervisory control is all the more significant. With regard to surveillance measures that constitute serious interferences with privacy, the principle of proportionality therefore places more rigorous demands on the effective design of this supervision both at the level of the law itself and in administrative practice (cf. BVerfGE 133, 277 <369 para. 214>). 140

To begin with, the guarantee of effective supervisory control requires a body vested with effective powers, such as, under current law, the Federal Data Protection Commissioner (see, fundamentally, BVerfGE 65, 1 <46>). It also requires to fully document the data collection. Technical and organisational measures must ensure that the data is available to the Federal Data Protection Commissioner in such a way that it can be evaluated in a practicable manner, and that the documents include sufficient information to match it with the process being overseen (BVerfGE 133, 277 <370 para. 215>). Since supervisory control has the function of compensating for a weak protection of the rights of the individual, it is particularly important that it be carried out regularly. Such supervision must be performed at reasonable intervals, the duration of which must not exceed a certain maximum of approximately two years. This must be taken into account with regard to the funding of the supervisory body (cf. BVerfGE 133, 277 <370 and 371 para. 217>). Guaranteeing compliance with the constitutional requirements for effective supervisory control is the joint responsibility of the legislature and the authorities (cf. BVerfGE 133, 277 <371 para. 218>). 141

e) Finally, to guarantee transparency and oversight, a legal rule on reporting duties is also needed. 142

Since covert surveillance measures occur largely unnoticed by persons concerned and the public, and since the obligation to notify or the right to information can only counteract this to a limited extent by offering the subsequent possibility of the protection of subjective rights, regular reports by the Federal Criminal Police Office to Parliament and to the public on the exercise of these powers must be required by law. These are necessary and must be sufficiently substantial in order to facilitate a public discussion on the nature and scope of data collected by means of these powers, including the handling of the obligations to notify or delete, and thus subject the data collection to democratic oversight and review (cf. BVerfGE 133, 277 <372 paras. 221 and 222>). 143

7. The provision of deletion requirements also belongs to the overarching proportionality requirements (cf. BVerfGE 65, 1 <46>; 133, 277 <366 para. 206>; established case-law). The purpose of these is to ensure that the use of personal data remains limited to the purposes that justified the data processing, and that the use is no longer possible once these have been achieved or settled. The deletion of the data must be documented in order to ensure transparency and oversight. 144

V.

In various respects, the challenged police surveillance measures do not satisfy the constitutional requirements set out above with regard to their respective conditions for interference. 145

1. § 20g sec. 1 to 3 BKAG is only partially compatible with the Constitution. 146

a) § 20g sec. 1 BKAG permits surveillance outside of private homes using the particular means of data collection defined in greater detail in § 20g sec. 2 BKAG. It thus authorises the Federal Criminal Police Office to interfere with the right to informational self-determination (Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG). 147

The provision, however, does not authorise interferences with Art. 10 sec. 1 GG. In contrast to §§ 20l, 20m BKAG, the powers listed in § 20g BKAG do not permit measures that interfere with the secrecy of telecommunications; nor do they permit measures that interfere with the right to the guarantee of the confidentiality and integrity of information technology systems, such as the manipulation of such systems for observation purposes. The provision is not to be measured against Art. 13 sec.1 GG either. It only authorises surveillance outside of private homes (cf. BTDrucks 16/9588, p. 23) and thus operates on the premise that the surveillance measures undertaken pursuant to it will, as must be ensured by technical means if need be, end at the doorstep. The powers of § 20g sec. 4 BKAG that reach beyond this are not subject-matter of these proceedings. 148

b) With regard to the weight of its interference, § 20g secs. 1 and 2 BKAG covers a wide spectrum, also encompassing serious interferences. 149

The provision permits surveillance outside of private homes using the means listed in section 2. Among these, in particular, are surveillance for extended periods, the covert creation of visual records, the covert monitoring of non-public speech, the application of tracking devices, or the use of police informants and undercover investigators. 150

The weight of interference of these measures can vary greatly. It extends from rather small to medium interferences, such as the taking of individual photographs or simple observation for a limited time, all the way to serious interferences such as the long-term on-going covert audio and visual recording of a person. Particularly when these measures are carried out together and thereby aim, with the help of modern technology, to register and audio-visually record as many utterances and movements as possible, they can constitute a particularly serious interference with privacy. 151

Similarly to the prevention of other weighty violations of legal interests or to the prosecution of significant criminal offences, the public interest in the effective prevention of terrorism can justify such interferences (see above, C II 3 a), provided that they are designed in a proportionate manner. This is, however, only partially the case here. 152

c) Deriving from general security law, the conditions for interference set out in in § 20g sec. 1 no. 1, sec. 2 BKAG are not objectionable. 153

aa) The provision limits the surveillance measures to the protection of sufficiently weighty legal interests. 154

Firstly, this applies insofar as it allows measures for the purpose of protecting the existence or the security of the state or the life, limb, or freedom of persons. In addition, the same applies to the extent that the provision allows measures aiming at the protection of property of substantial value the preservation of which is in the public interest. A reasonable interpretation of this will not include the preservation merely of significant material assets. Rather, in the regulatory context of the protection against terrorism, this will be taken to mean significant infrastructure facilities or other sites of direct importance for society (vgl. BVerfGE 133, 277 <365 para. 203>). 155

Pursuant to § 20g sec. 1 no. 1 BKAG, the powers to interfere are also further restricted in that measures for the protection of the legal interests mentioned above are only permitted when these are threatened by one of the criminal offences listed in § 4a sec. 1 sentence 2 BKAG. This is evident in function provision of § 4a BKAG itself into which the powers of §§ 20a et seq. BKAG are integrated. The powers to interfere are 156

thus restricted to the protection against threats from international terrorism. Here, the legislature does not merely refer to the unspecific term “terrorism”, nor to §129 StGB in general, but rather it specifies that the threat to legal interests must emanate from specific criminal offences that are individually defined and particularly qualified in § 129a StGB. The provision is thus restricted to the protection of particularly weighty legal interests against particularly threatening attacks. Leaving aside the question of where the constitutional limits generally lie in respect of such measures – for example, also in terms of the corresponding powers under the Police Acts of the *Laender* –, the proportionality requirements are met at any rate in the case at hand.

In contrast, the reference in § 20g sec. 1 no. 1 BKAG to the legal definition of “threat” in § 20a sec. 2 BKAG cannot be understood to mean that § 20a sec. 2 BKAG overrides the limitation of the legal interests in § 20g sec. 1 no. 1 BKAG and assumes that any threat to public security arising in the context of criminal offences pursuant to § 4a sec. 1 sentence 2 BKAG is sufficient. § 20a sec. 2 BKAG does indeed specify the term “threat”, as applying to all powers listed thereafter, and by highlighting the requirement that it must arise in an individual case. Yet, under a reasonable and constitutionally required interpretation, the function of this provision is not to override the specifically limited requirements pertaining to the protection of legal interests as they apply to individual powers. 157

bb) § 20g sec. 1 no. 1 BKAG also requires sufficiently specified grounds for ordering the measures. The provision requires the presence of a threat. Pursuant to § 20g sec. 2 BKAG this is to be understood as an “existing threat in an individual case” and thus as “a specific threat” within the meaning of general security law. In light of the regular courts’ jurisprudence shaping this term, there are no grounds for objections on the basis of specificity or proportionality considerations. 158

cc) Furthermore, there are no constitutional objections to the fact that § 20g sec. 1 no. 1 BKAG determines the persons addressed by the measures by reference to §§ 17, 18 and 20 of the Act on the Federal Police (*Bundespolizeigesetz* – BPolG) and thus to principles of responsibility under police laws. The legislature is permitted to resort to the institutions of general security law. […] With regard to the powers of § 20g secs. 1 and 2 BKAG in question here, which neither interfere with Art. 10 sec. 1 GG, nor with the right to the guarantee of the confidentiality and integrity of information technology systems, nor with Art. 13 sec. 1 GG, there is also no objection to be made on the basis that surveillance pursuant to § 20 BPolG can also be ordered with regard to a person from whom the threat does not emanate, under the same conditions required for state of necessity duties. The provisions to this effect are narrowly defined and are to be interpreted strictly. […] 159

dd) The means of surveillance defined in § 20g sec. 2 BKAG are also not too unspecific or disproportionate. However, these powers also include – irrespective of the different weight of the individual interferences – particularly serious interferences, such as the possibility of long-term audio and visual recording of private conversations and situations, or the taking advantage of trust by undercover investigators and police informants. In order to protect against the particularly serious threats named in § 20g sec. 1 no. 1 BKAG, though, these serious interferences may also – in accordance with a test of proportionality carried out in the individual case – be constitutionally justified. 160

The technologically open definition of the means of surveillance of § 20g sec. 2 nos. 2 and 3 BKAG does not meet with any objections either. The legislature is not obligated to limit the authorised means of surveillance to the technological state of the art at the point in time of the legislative process. As long as the type of surveillance that is permitted can be sufficiently made out, the legislature can provide that the authorisation shall also cover future technological developments. […] Furthermore, it falls upon the legislature to carefully observe technological developments and to take appropriate corrective action if the specific defining of openly phrased legal terms takes an undesirable turn (cf. BVerfGE 112, 304 <316 and 317>). 161

d) § 20g sec. 1 no. 2 BKAG, however, is not compatible with the constitutional requirements. The conditions for interference neither satisfy the principle of specificity nor the principle of proportionality in the narrow sense. 162

aa) § 20g sec. 1 no. 2 BKAG complements the basis for interference of § 20g sec. 1 no. 1 BKAG, which is limited to the protection against threats. It is intended by the legislature to set in earlier and serve to prevent criminal offences. 163

According to the standards set out above, the legislature is not generally prevented nor constitutionally barred from limiting security measures to the protection against – according to established understanding – specific threats. However, even in respect of measures for preventing criminal offences, a prognosis is needed that is based on facts relating to a specific threat, rather than merely on general experience. In principle, this means that an occurrence that is specific at least with regard to its type, and temporally foreseeable, must be in evidence (cf. BVerfGE 110, 33 <56 and 57, 61>; 113, 348 <377 and 378>; 120, 274 <328 and 329>; 125, 260 <330>). In respect of terrorist offences, the legislature can alternatively also apply the standard of whether the individual behaviour of a person substantiates the specific probability that the person will commit a terrorist offence in the near future (see above, C IV 1 b). The requirements to this effect must be set out with legal clarity. 164

bb) § 20g sec. 1 no. 2 BKAG does not satisfy these standards. The provision does indeed require the possible commission of a terrorist offence. Yet the prognosis requirements to this effect are not sufficiently substantive. The provision does not preclude the possibility that the prognosis is solely based on general experience. It neither contains the requirement that an occurrence that is specific at least with regard to its type and temporally foreseeable must be in evidence, nor the alternative that the individual behaviour of a person must substantiate the specific probability that the person will commit a terrorist offence in the near future. Thus, the provision does not give the authorities and the courts sufficiently specific criteria to work with and provides for measures that can be disproportionately broad. 165

e) If interpreted in conformity with the Constitution, there can, in contrast, be no constitutional objection to § 20g sec. 1 no. 3 in conjunction with § 20b sec. 2 no. 2 BKAG. 166

§ 20g sec. 1 no. 3 BKAG also allows measures affecting contacts or accompanying persons. The term “contacts or accompanying persons” is defined in greater detail in § 20b sec. 2 no. 2 BKAG and is to be understood, when construed appropriately, as an umbrella term solely for the groups of persons designated in it. 167

With this proviso, § 20g sec. 1 no. 3 BKAG is constitutionally sound. The legislature does not indiscriminately open up the possibility of carrying out surveillance of all persons in the target person’s sphere, in order to – based merely on the fact that there has been contact with that person – then find out whether this will uncover evidentiary bases for further investigations. Rather, for the ordering of measures targeting third parties, the provision requires that they have a particular proximity to the offence defined in greater detail in § 20b sec. 2 no. 2 BKAG. […] 168

There are also no objections to be raised with regard to the individual criteria set out in § 20b sec. 2 no. 2 a to c BKAG. Certainly, for constitutional reasons, the criteria cannot be understood as being limitlessly broad so as to include persons who had economic relations with the target person long before any criminal offence. Rather, § 20b sec. 2 no. 2 b BKAG limits the obtained benefits to the exploitation of the offence and thus to the fruit that stems from its unjust nature, while § 20b sec. 2 no. 2 c BKAG also requires that the instrumentalisation of the person concerned must be closely connected to the offence itself. If these conditions are fulfilled, the relevant orders are constitutionally justified. This is not altered by the fact that these measures can thus also target third parties acting in good faith who are not responsible for any threat. While this does constitute a particularly serious interference, it is a constitutionally justified means in the context of exceptionally significant public interests, similar to obligations of witnesses or duties in a state of necessity. 169

f) As far as the principle of proportionality is concerned, the procedural requirements of § 20g sec. 3 BKAG are not sound in all respects. 170

aa) It is not objectionable that the surveillance measures under this provision, each of which may be ordered for a reasonably limited period of time only, can be extended without this being subject to any maximum limit. The legislature could assume that a specific risk situation, as is required for the ordering or extension of the measures, generally does not last over a long period of time, so that there is, generally, no risk that this will lead to disproportionate on-going surveillance. Furthermore, a limit can be imposed, based on the principle of proportionality in individual cases even if no maximum limit is expressly set down, since the longer the surveillance measures, the more intensive the interference with the general right of personality, which may render a further renewal constitutionally unjustifiable (cf. BVerfGE 109, 279 <362>). 171

bb) With regard to proportionality aspects, however, the rule on the requirement of a judicial order in § 20g sec. 3 BKAG is insufficient. 172

§ 20g sec. 3 BKAG requires a direct judicial order for the initial ordering of a measure only if undercover investigators are to be employed (cf. § 20g sec. 3 sentence 1 BKAG). In other cases, it permits an initial order directly from the Federal Criminal Police Office itself and requires a judicial decision only for a potential extension (§ 20g sec. 3 sentence 8 BKAG). This applies, on the one hand, with respect to the monitoring and recording of non-public speech and the use of police informants or undercover investigators (§ 20g sec. 2 nos. 2 b, 4 and 5 BKAG), as well as, on the other hand, long-term observation (§ 20g sec. 2 no. 1 BKAG), which also includes those cases in which it is carried out by means of visual recordings or the use of technical means such as tracking devices (cf. § 20g sec. 2 nos. 2 a and 3 BKAG). 173

This provision only partially satisfies the constitutional requirements. It is, however, not objectionable that image recording as well as merely short-term observations – even using visual recording or technical means such as tracking devices – are not subject to a judicial order. Should the surveillance measures remain limited in this manner, then the weight of their interference is not so significant as to constitutionally require a judicial order (cf. stricter with regard to observation by means of a GPS tracker, Supreme Court of the United States, United States v. Jones, 132 S. Ct. 945 [2012]; on the surveillance of a suspect by means of GPS, more reserved on the other hand, ECtHR, Uzun v. Germany, judgment of 2 September 2010, no. 35623/05, para. 70, NJW 2011, p. 1333 <1336 and 1337>, on Art. 8 ECHR). In contrast, an independent review is constitutionally indispensable if observations within the meaning of § 20g sec. 3 no. 1 BKAG are to be carried out over a longer period of time – particularly when this involves visual recording or the use of particular technical means such as tracking devices –, if non-public speech is to be monitored or if police informants are to be used. These measures constitute such a serious interference with privacy that their ordering must be reserved for an independent body, such as a court. In this respect, it is not sufficient to permit the security authority to initially order the measures itself but to provide for the disciplinary effect of a judicial decision – possibly on the basis of the information thus obtained – only at the renewal stage. To the extent that it is provided that the initial ordering of these measures may occur without a judicial decision, the procedural design of § 20g BKAG is not proportionate. 174

g) § 20g BKAG is also insufficient with regard to the constitutional requirements insofar as it does not provide for any protection of the core area of private life. 175

§ 20g BKAG authorises surveillance measures of varying quality and proximity to privacy. By also permitting long-term visual recording and long-term monitoring and recording of non-public speech, the provision authorises surveillance measures that typically constitute a serious interference with privacy. These measures all involve surveillance taking place outside of private homes. Yet this does not mean that – be it in the car, be it sitting separately in a restaurant, be it secluded on a stroll – highly confidential situations belonging to the core area of private life are not likely to be recorded […]. 176

With regard to certain powers, the provision thus has a proximity to the core area that makes an express legal provision for the protection of the core area of private life necessary. The legislature must, in a clear manner, provide for protective provisions both with regard to data collection as well as with regard to data analysis and use (see above, C IV 3 c bb, d). Such provisions are lacking, so that § 20g secs. 1 and 2 BKAG are not compatible with the Constitution in that respect either. 177

2. § 20h BKAG, too, only partially satisfies constitutional requirements. 178

a) § 20h BKAG permits audio and visual surveillance in private homes. It thus constitutes an interference with Art. 13 sec. 1 GG. 179

With the power to conduct surveillance within private homes, the provision authorises interferences with fundamental rights that are particularly serious. It permits the state to penetrate into spaces that are a person's private refuge and that are closely linked to human dignity (cf. BVerfGE 109, 279 <313 and 314>). This does not, as implied by Art. 13 secs. 3 and 4 GG, rule out surveillance measures. The protection against threats from international terrorism may justify such measures (see above, C II 3 a). These are, however, subject to particularly strict requirements, which § 20h BKAG does not fulfil in every respect. 180

b) § 20h secs. 1 and 2 BKAG is not constitutionally objectionable insofar as it – comprehensively, with regard to all persons potentially addressed – governs the general conditions for the surveillance of private homes. 181

aa) The provision does satisfy constitutional requirements insofar as it limits measures to the protection of particularly weighty legal interests, and at the same time requires the presence of imminent danger, and defines the persons addressed by it as those responsible for particular actions or circumstances. 182

[…] 183

bb) In accordance with Art. 13 sec. 4 GG, the provision also requires the presence of imminent danger. For this, both the extent as well as the probability of the damage to be expected must be considered (cf. BVerfGE 130, 1 <32>). Strict requirements, going beyond those needed in relation to a specific threat, must be laid down with regard to the presence of imminent danger (cf. BVerwGE 47, 31 <40>; Decisions of the Federal Court of Justice in Criminal Matters – *Entscheidungen des Bundesgerichtshofs in Strafsachen* – BGHSt 54, 69 <83 and 84>). From a proportionality perspective, this does ensure sufficiently specific grounds for carrying out such measures (see above, C IV 1 b). 184

cc) The provision is also not disproportionate for permitting audio as well as visual surveillance of private homes. The fact that the Constitution does not already fundamentally rule out visual surveillance of private homes for interferences serving to protect against threats pursuant to Art. 13 sec. 4 GG can be deduced *a contrario* from Art. 13 sec. 3 GG. However, interference combining audio and visual surveillance carries substantially more weight than, for example, audio surveillance only, and requires special justification. Accordingly, when ordering these measures, the suitability, necessity and appropriateness requirements for each form of surveillance must be examined individually, as well as with a view to their combination with one another, where applicable. It will normally not be sufficient for the additional ordering of visual surveillance to cite merely the increased ease at matching voices; rather, more significant grounds relevant to the success of the surveillance are needed. In the context of applying the law, these requirements can and must be taken into consideration. § 20h sec. 1 nos. 1 and 2 BKAG, which lays down audio and visual surveillance of private homes as separate surveillance measures which must therefore be examined separately, provides a sufficient basis for this. 185

c) The definition of the persons potentially addressed by the surveillance measures, however, is partially disproportionate and incompatible with the Constitution. 186

aa) There is nothing to object to with regard to § 20h sec. 1 no. 1 a BKAG, which provides for the authorisation to order the surveillance of private homes targeting persons responsible within the meaning of §§ 17, 18 BPolG (see above C IV 1 c). 187

There is also no cause for objection in that § 20g sec. 2 BKAG thereby permits the surveillance of such persons not only in their own home but also in the home of third parties, if the target persons are present and measures in the home of the target person alone would not lead to protection against the danger. However, the Federal Constitutional Court has formulated restrictive standards of interpretation with regard to such surveillance measures in the homes of third parties […] (cf. BVerfGE 109, 279 <356 and 357>). 188

bb) § 20h sec. 1 no. 1 b BKAG, which permits the surveillance of private homes with respect to persons whose involvement in specific preparations justify the assumption of the commission of terrorist offences, is constitutionally sound. 189

Unlike § 20g sec. 1 no. 2 BKAG, the provision does not create separate grounds for interference applying particularly far ahead of the time of the danger. Instead, it requires – in accordance with Art. 13 sec. 4 GG – imminent danger to qualified legal interests for whose protection the surveillance must be necessary. Moreover, the class of persons addressed by these measures is sufficiently limited: By requiring knowledge of specific preparations of – more narrowly qualified – terrorist offences, the provision stipulates the existence of an occurrence that is specific with regard to its type and temporally foreseeable. In doing so, it provides a basis for carrying out such measures that satisfies the constitutional requirements (see above, C IV 1 b). 190

cc) The authorisation of the surveillance of private homes with regard to contacts or accompanying persons (§ 20h sec. 1 no. 1 c BKAG), however, is incompatible with Art. 13 secs. 1 and 4 GG. It is disproportionate. 191

The surveillance of private homes is a particularly serious interference with privacy. By its nature, it has a more serious impact than surveillance measures outside of private homes or than telecommunications surveillance. The weight of its interference is paralleled only by interferences with information technology systems. For this reason, the appropriateness of such a measure can only be ensured if it is restricted from the outset to exclusively capturing conversations of the target person responsible for the threat (cf. BVerfGE 109, 279 <355>). Directly extending these measures to third parties is disproportionate and is to be ruled out with regard to such a serious interference (see above C IV 1 c). 192

This does not affect the fact that it is permissible for the surveillance of the private home of the target person to also include non-involved third parties so long as this is inevitable (cf. § 20h sec. 2 sentence 3 BKAG). It is even permissible, as explained, to carry out surveillance of the private homes of third parties in order to carry out surveillance of the target person. 193

d) There is no constitutional objection to be raised with regard to the surveillance of private homes in terms of its procedural design. In particular, it is to be ordered by a judge. The fact that the Act thereby requires an indication of the “material grounds” (§ 20h sec. 4 no. 4 BKAG) – as required in the other corresponding provisions of the Act, too (cf. § 20k sec. 6 no. 4 BKAG) – does not constitute a revocation of the constitutional duty to review and the duty to justify (cf. BVerfGE 109, 279 <359 and 360>), but rather emphasises that all legally relevant aspects must be substantiated in a sound manner. 194

It is also constitutionally unobjectionable that there is no maximum limit for the number of times the order for the surveillance of private homes can be extended, since a temporal limit can, if needed in an individual case, arise on the basis of proportionality considerations (cf. BVerfGE 109, 279 <362>). 195

e) The provisions on the protection of the core area of private life in § 20h sec. 5 BKAG are not constitutionally sufficient. They do not satisfy the requirements of Art. 13 sec. 1 in conjunction with Art. 1 sec. 1 GG. 196

aa) Since the surveillance of private homes is a particularly serious interference with privacy and an intrusion into individuals’ personal refuges which are particularly important for safeguarding human dignity, the related requirements for the protection of the core area are particularly strict (BVerfGE 109, 279 <313 et seq., 318 et seq., 328 et seq.>). 197

(1) Firstly, particular requirements apply at the level of the collection of data. When weighing whether there is a probability that highly private situations will be recorded, presumptions shall apply in the interest of an effective protection of the core area (cf. BVerfGE 109, 279 <320>). Accordingly, conversations taking place in private spaces with persons enjoying the highest level of personal trust (see above, C IV 3 a) are presumed to fall within the core area of private life and cannot be subject to surveillance (cf. BVerfGE 109, 279 <321 ff.>). An automatic on-going surveillance of spaces in which such conversations are to be expected must thus be ruled out (cf. BVerfGE 109, 279 <324>). This presumption can be refuted when specific indications suggest that certain conversations are, within the meaning of the standards set out above, directly related to a criminal offence – a relation that exists even when the conversations are mixed with highly personal content, or if their overall character will not be highly confidential. The mere prognosis, however, that highly confidential and everyday matters will be combined in a conversation is not sufficient (cf. BVerfGE 109, 279 <330>, see above, C IV 3 a, d). 198

If, considering the above, there is a probability that a surveillance measure will interfere with the core area of private life, the measure may not be carried out. If – also taking into account rules of presumption – there are no indications that there will be an intrusion into the core area of private life, the measures may be carried out. However, should highly confidential situations nevertheless be recorded, the measures must be discontinued immediately (cf. BVerfGE 109, 279 <320, 323 and 324>). If there are doubts – for linguistic reasons, for example – as to the highly confidential nature of a situation, or specific reasons to believe that together with the exchange of highly private thoughts criminal offences are also being discussed, then the surveillance may be continued in the form of automatic recording. 199

(2) Specific constitutional requirements also arise at the level of data analysis and data use. It must be provided that the results of the surveillance will be screened by an independent body. This screening serves both as a review of legality as well as a filtering out of highly confidential data, so that – as far as possible – it is not disclosed to the security authorities. The independent body is to be provided with all the data resulting from the surveillance of private homes (cf. BVerfGE 109, 279 <333 and 334>; differently Chamber Decisions of the Federal Constitutional Court – *Kammerentscheidungen des Bundesverfassungsgerichts* – BVerfGK 11, 164 <178>). 200

In the case that, despite all safeguards, information relevant to the core area is collected, both a prohibition of its use, as well as a deletion requirement, including the documentation of the deletion, must be put in place (see above, C IV 3 c bb, d, 7). 201

bb) On this basis, § 20h sec. 5 BKAG satisfies the constitutional requirements at the data collection level, but not at the level of its use. 202

(1) For the surveillance of private homes, § 20h sec. 5 sentences 1, 2, 3 and 5 BKAG requires an examination of whether information from the core area will be collected. By allowing surveillance only under the presumption, based on a prognosis, that any expression that is to be attributed to the core area of private life may not be collected and that the measures will be stopped if, contrary to the prognosis, the surveillance of private homes provides reasons to believe that highly private information is being collected, the provision satisfies constitutional requirements. This also applies to the authorisation to record automatically pursuant to sentence 3, which does not set aside the legality requirements of sentence 1, but rather ties in with the interruption of monitoring and observation of individual persons required by sentence 2. Where § 20h sec. 5 sentence 1 BKAG protects “expressions” relevant to the core area, this also includes, when construed appropriately, visual recordings of equivalent situations. 203

(2) At the level of data use, however, the approach with regard to the protection of the core area does not satisfy the constitutional requirements in every respect. The Act provides for a screening of the recordings by a court, yet it limits this screening to automatic recordings in respect of which doubts have arisen (§ 20h sec. 5 sentence 4 BKAG). Insofar, the legislature is clearly guided by the consideration that further independent screening is not necessary, because the collection of highly personal information is ruled out at the collection level by § 20h sec. 5 sentences 1 and 2 when the Act is properly applied. This 204

does not, however, justify such a limit to the independent screening of recordings from the surveillance of private homes. For the aim of such screening is not solely filtering cases of doubt but also to guarantee an independent review with regard to the requirements that serve to protect the core area in general. The courts' only limited power to review pursuant to § 20h sec. 5 sentence 4 BKAG, however, does not guarantee this.. Indeed, the Basic Law gives the legislature sufficient leeway to provide for special rules applicable exceptional cases in case of immediate danger when designing the review powers.

In accordance with the constitutional requirements, for highly personal data that is nevertheless collected, the legislature has indeed provided for a prohibition of use and its immediate deletion, as well as a documentation of the deletion. What is unconstitutional, however, is the very short period of time in § 20h sec. 5 sentence 10 BKAG during which the deletion logs are to be deleted. This period is so brief that during the storage period of the deletion logs typically neither a review by the Federal Data Protection Commissioner nor by the party concerned is likely to occur and the documentation of the deletion thus becomes meaningless (cf. Bäcker, loc. cit., p. 88; cf. in this respect also BVerfGE 100, 313 <400>; 109, 279 <332 and 333>). Since the deletion logs themselves do not contain any data that might incriminate the person concerned, this brief period in particular cannot be justified on the grounds that it serves to protect this person. 205

3. The conditions set out for electronic profile searching pursuant to § 20j BKAG are constitutionally unobjectionable. 206

The provision provides the basis for an interference with the right to informational self-determination. Yet the conditions for interference are sufficiently specific and proportionate in their design, so that the interference is justified. In particular, electronic profile searching is permitted for the protection of sufficiently weighty legal interests (see above, C V 1 c aa) and requires a specific threat pursuant to § 20j sec. 1 sentence 1 in conjunction with § 20a sec. 2 BKAG. There can be no constitutional objection either to the example in the second half of § 20j sec. 1 sentence 1 BKAG, in which the legislature specifies the required risk situation exemplarily. The relevant requirements (cf. BVerfGE 115, 320 <363 et seq.>) remain unaffected by this. The provision is also proportionately designed in procedural respects; in particular, it requires a judicial order. 207

4. § 20k BKAG, if interpreted in conformity with the Constitution, is constitutional with regard to the general conditions for interference. However, the rules with regard to the protection of the core area of private life do not satisfy the constitutional requirements. 208

a) § 20k sec. 1 BKAG authorises access to information technology systems and permits covert remote searches of information technology systems, by means of which data saved or stored on the affected person's private computer or other computers linked thereto (for example in "the cloud") can be collected and the person's online behaviour can be tracked. The provision thus permits interference with the fundamental right to the guarantee of the confidentiality and integrity of information technology systems (Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG). 209

With this stand-alone manifestation of the general right of personality, the Constitution takes account of the significance of the use of information technology systems, which nowadays reaches deep into privacy, for the development of personality (cf. BVerfGE 120, 274 <302 et seq.>). Today, diary-like written expressions, intimate statements, or other written manifestations of highly personal experience, film or audio recordings are increasingly generated, saved and in part exchanged in electronic form. A large part of highly personal communication takes place electronically by means of communications services over the internet or in the context of internet-based social networks. This data, whose confidentiality the persons concerned depend upon and trust in, is largely no longer to be found on personal information technology systems alone but rather on that of third parties. The fundamental right to the guarantee of the confidentiality and integrity of information technology systems therefore protects against covert access to this data, and thus in particular against remote searches whereby private computers as well as other information technology systems are manipulated and read, and whereby personal data stored on external 210

servers with a reasonable expectation of confidentiality is accessed and movements on the web of the persons concerned are tracked. Given the often highly personal nature of this data, which arises in particular when it is taken as a whole, this constitutes a particularly intense interference with this fundamental right. Its weight is commensurable with that of an interference with the inviolability of the home.

b) The requirements of § 20k secs. 1 and 2 BKAG with regard to access to information technology systems, when interpreted in conformity with the Constitution, satisfy the constitutional requirements. 211

aa) Interferences with the right to the guarantee of the confidentiality and integrity of information technology systems, however, are subject to strict conditions (cf. BVerfGE 120, 274 <322 et seq., 326 et seq.>). Specifically, the measures must be contingent on factual indications that a specific impending danger to an exceptionally significant legal interest is present in the individual case. § 20k sec. 1 BKAG satisfies this requirement. […] 212

§ 20k sec. 1 sentence 2 BKAG, however, must be subject to a restrictive interpretation in conformity with the Constitution. The possibility presented in this provision of carrying out measures in advance of a specific danger if certain facts indicate that, in an individual case, an impending danger of a terrorist offence is present is to be interpreted in such a way that such measures are only permitted if the facts indicate an occurrence that is specific at least with regard to its type and that is temporally foreseeable, and if it is clear that specific persons will be involved and their identity is sufficiently determined for surveillance measures to be carried out with respect to and largely limited to them (BVerfGE 120, 274 <329>). It is also sufficient if an occurrence is not specific at least with regard to its type and not temporally foreseeable yet the individual behaviour of the person concerned substantiates the specific probability that the person will commit such offences in the near future (see above, C IV 1 b). 213

Since § 20k sec. 1 sentence 2 BKAG is drafted in accordance with the case-law of the Federal Constitutional Court (BVerfGE 120, 274 <329>), it can be presumed that the legislature intended to refer to it. The provision can thus still be interpreted in a manner that is compatible with the Constitution. 214

bb) Furthermore, in respect of the substantive conditions for interference, the provision satisfies the principle of proportionality. In particular, § 20k sec. 2 BKAG provides that changes to the information technology system caused by the access must be minimised, the use of the access by third parties must be prevented, and at termination it must be reversed to the greatest extent possible (cf. in this respect BVerfGE 120, 274 <325 and 326>). The fact that consequential damage cannot be ruled out entirely does not render the measure disproportionate from the outset. Respect for the principle of proportionality in individual cases also means that open access to a target person's data sets must generally be given priority over covert infiltration. 215

c) Moreover, there are no objections to the procedural design of the provision (cf. § 20k secs. 5 and 6 BKAG). A measure may only be ordered by a judge and the order requires substantive reasoning (cf. BVerfGE 120, 274 <331 et seq.>; see above, C IV 2). The measure can be ordered for a long period of up to three months. This is constitutionally sound only on condition that this be a maximum time limit for each order and the actual duration of the order be determined by a test of proportionality in the individual case. 216

d) The provisions for the protection of the core area of private life, however, do not satisfy the constitutional requirements in every respect. 217

aa) Given that covert access to information technology systems typically carries with it the risk of the collection of highly confidential data, and thus is in particular proximity to the core area, it requires express legislative safeguards for the protection of the core area of private life (cf. BVerfGE 120, 274 <335 et seq.>). The relevant requirements are not identical in every respect to those that apply to the surveillance of private homes, and shift the protection away from the collection level to the subsequent analysis and use level (cf. BVerfGE 120, 274 <337>). The reason for this lies in the specific nature of access to information technology systems. Here, protective measures to prevent violations of the core area do not 218

aim primarily at preventing the collection and recording of a fleeting, highly confidential moment in a private space, but rather at preventing the reading of highly confidential information within a comprehensive data set of digital information that already exists, and that, taken as a whole, is typically not of a private nature the way behaviour or communication in a home would be. Here, the surveillance does not take place in the form of a chronologically ordered occurrence in different locations, but rather as access by means of a spy program which, as far as the access is concerned, presents only the alternatives of all or nothing.

The requirements for the protection of the core area have thus to a certain extent been cut back. 219
However, even here, it must be provided that the collection of information that can be considered to belong to the core area does not take place to the extent that this is possible from a technical and investigative standpoint. Available information technology safeguards in particular are to be used; if these can detect and isolate highly confidential information, access thereto is prohibited (cf. BVerfGE 120, 274 <338>).

If, however, data relevant to the core area cannot be filtered out before or at the time of the data 220
collection, access to the information technology system is nevertheless permissible even if it is probable that highly personal data too might incidentally be collected. In this respect, the legislature must take into account the need for protection of the person concerned by putting in place safeguards at the levels of analysis and use, and by minimising the effects of such access. Decisive significance attaches to the screening by an independent body that filters out information relevant to the core area prior to its availability to and use by the Federal Criminal Police Office (cf. BVerfGE 120, 274 <338 and 339>).

bb) § 20k sec. 7 BKAG only partially satisfies these requirements. 221

(1) The requirements applicable at the level of data collection, however, are unobjectionable if 222
interpreted in conformity with the Constitution. The second sentence of the provision, in conformity with the aforementioned requirements, provides that all technically available means must be used to prevent the collection of information relevant to the core area. Furthermore, the provision prohibits access to information technology systems solely in cases where “only” information from the core area of private life is collected. According to the standards presented above, this is constitutionally sound. For constitutional reasons, the provision, however, must be interpreted in such a manner that communication on highly confidential matters is not excluded from the strict protection of the core area merely because it combines highly confidential with everyday matters (cf. BVerfGE 109, 279 <330>). In this respect, the provision is to be interpreted and applied in conformity with the constitutional requirements for the protection of the core area of private life and in light of the relevant understanding of the concept (see above, C IV 3 a, d).

(2) In contrast, the measures in question lack constitutionally sufficient safeguards at the level of a 223
subsequent protection of the core area. § 20k sec. 7, sentences 3 and 4 BKAG do not provide for sufficiently independent review.

The constitutionally required screening by an independent body serves not only as a review of legality, 224
but also significantly as a way of filtering out data relevant to the core area of private life so that, where possible, it remains undisclosed to the security authorities. This presupposes that the review is largely conducted by external persons not charged with security tasks. This does not rule out the involvement of an employee of the Federal Criminal Police Office – subject to a separate duty of confidentiality – in order to ensure expertise in a specific investigative matter. Moreover, in a similar manner, the Federal Criminal Police Office can offer technical support - including, for example, for language mediation purposes - for the screening. Yet the actual carrying out and decision-making responsibility must remain in the hands of persons who are independent with regard to the Federal Criminal Police Office.

This is not ensured by the current statutory approach. It largely entrusts the Federal Criminal Police 225
Office itself with the screening. The fact that one of the employees, such as the Federal Data Protection Commissioner within this specific public authority, is not subject to instruction does not mitigate this issue; nor does subjecting the screening to the general “expert oversight” of the ordering court.

By contrast, § 20k sec. 7 sentences 5 to 7 BKAG ensures further safeguards at the level of use for an effective protection of the core area in a constitutionally sound manner. What is unconstitutional here too, however, is the very short period of time in § 20k sec. 7 sentence 8 BKAG, during which the deletion logs must be retained (see above, C IV 3 d). 226

5. § 20l BKAG is only partially compatible with the Constitution. 227

a) § 20l BKAG governs telecommunications surveillance and thus provides a basis for interferences with Art. 10 sec. 1 GG. In that respect, Art. 10 sec. 1 GG is not only the relevant standard with regard to § 20l sec. 1 BKAG, which governs the conventional surveillance of telecommunications, but also with regard to § 20l sec. 2 BKAG, which allows telecommunications surveillance at the source insofar as technical measures ensure that the surveillance only covers on-going telecommunications. While this technically requires having access to the respective information technology system, § 20l sec. 2 BKAG only allows those surveillance measures that are limited to on-going telecommunications processes. Thus, the purpose of the provision is merely to track the technological developments in information technology and to allow – without accessing further content-related information provided by the information technology system – telecommunications surveillance also in those cases in which it is no longer possible by means of the old surveillance technology. As a result, this measure must not be evaluated in the light of the fundamental right to the guarantee of the confidentiality and integrity of information technology systems but rather with a view to the standards set out in Art. 10 sec. 1 GG (cf. BVerfGE 120, 274 <309>). 228

Telecommunications surveillance entails interferences that are serious (cf. BVerfGE 113, 348 <382>; 129, 208 <240>). However, they are justified for the purpose of protecting against threats from international terrorism (see above, C II 3 a) insofar as the grounds for the interference are proportionately restricted in the individual case. § 20l BKAG, however, only partially ensures that this is the case. 229

b) § 20l sec. 1 nos. 1 to 4 BKAG provides different grounds for interferences with regard to different addressees. Not all of them satisfy the constitutional requirements. 230

The authorisation to carry out surveillance measures against those persons deemed to be responsible under police laws pursuant to § 20l sec. 1 no. 1 BKAG does not raise constitutional concerns as it in fact also aims to protect qualified legal interests and has the sole purpose of providing protection against imminent dangers. 231

However, in contrast, the not specifically limited extension of telecommunications surveillance under § 20l sec. 1 no. 2 BKAG to also cover persons regarding whom certain facts justify the assumption that they are preparing terrorist crimes is not compatible with the Constitution. The provision, which shifts interference powers beyond the prevention of a specific threat to an earlier stage with the aim of preventing criminal offences, violates, given its ill-defined open phrasing, the principle of legal certainty and is disproportionately broad. In this respect, the same considerations as developed with regard to § 20g sec. 1 no. 2 BKAG (see above, C V 1 d) apply here, too. The marginally different formulations of the two provisions do not imply any difference in substance. This is also clarified by the Act's explanatory memorandum that partially paraphrases the content of § 20l sec. 1 no. 2 BKAG by using those words that were also used by the legislature in § 20g sec. 1 no. 2 BKAG (cf. BTDrucks 16/10121, p. 31). The same applies insofar as § 20l sec. 2 BKAG contains a reference to that provision. 232

In contrast, the possibility of extending telecommunications surveillance to also cover messengers pursuant to § 20l sec. 1 nos. 3 and 4 BKAG is, when interpreted in conformity with the Constitution, compatible with Art. 10 sec. 1 GG. The provision, formulated closely in line with § 100a sec. 3 Code of Criminal Procedure (*Strafprozessordnung* – StPO), is sufficiently open to interpretation and satisfies the requirements of the principle of legal certainty. Like the rules on contacts and accompanying persons set out in § 20b sec. 2 no. 2 BKAG, this provision does not allow indiscriminately extending surveillance measures to all persons that have exchanged messages with the target person, but rather requires that 233

there be specific grounds – that are to be set forth in the order accordingly – indicating that the target person is involving the messenger in the realisation of a criminal offence and that the latter is thus particularly closely linked to a crime or threat.

c) The additional further conditions under which § 20l sec. 2 BKAG allows, subsidiarily, telecommunications surveillance at the source do not raise effective constitutional concerns. […] 234

d) Procedurally, and in accordance with the constitutional requirements, § 20l sec. 3 BKAG sets out the requirement of a judicial order (cf. BVerfGE 125, 260 <337 and 338>). However, it lacks a statutory rule that stipulates – as required under constitutional law (see above, C IV 2) – that the order for telecommunications surveillance informs of the grounds for this measure. This cannot be overcome by means of an interpretation in conformity with the Constitution. In light of the fact that the Act expressly sets out obligations to provide explanatory statements in other provisions (cf. § 20g sec. 3 sentence 6, § 20h sec. 4, § 20k sec. 6 BKAG), an interpretation here in the sense that the absence of a rule requiring that the reasons be communicated is based on an intentional decision to that end cannot be ruled out with sufficient certainty. 235

e) The provisions on the protection of the core area of private life pursuant to § 20l Abs. 6 BKAG are for the most part compatible with the Constitution. 236

aa) Telecommunications surveillance constitutes a serious interference that is in particularly close proximity to the core area. As a form of content-related surveillance of all kinds of telecommunications-based exchanges, it typically entails the risk of also collecting highly private communication that is subject to the protection of the core area of private life. Insofar, special legislative protective precautions are needed (cf. BVerfGE 113, 348 <390 and 391>; 129, 208 <245>). 237

However, telecommunications surveillance is, considering its overall character, not defined by an intrusion into privacy to the same extent as the surveillance of private homes or remote searches might be (cf. BVerfGE 113, 348 <391>). It covers any kind of communication in any situation, as long as it is transmitted by technical means. Highly confidential communication is indeed one small component that is under threat of being covered by the surveillance measures, too; however, it is not – unlike in the case of the surveillance of a person's private refuge in a private home – a distinctive feature. In that respect, it is also different from remote searches. […] Its proximity to the core area of private life lies mainly in the fact that it also covers highly personal communication between highly trusted persons (cf. BVerfGE 129, 208 <247>). 238

The legislature can take this into account by stipulating less stringent requirements for the protection of the core area. However, this too requires an assessment – to be taken at the collection stage – as to whether it is likely that highly private conversations will be covered, the surveillance of which must thus be prohibited if necessary. Provided such conversations cannot be identified with sufficient probability, the surveillance measure may be carried out – and, in accordance with a proportionality test, also by means of automatic on-going surveillance in the individual case (cf. BVerfGE 113, 348 <391 and 392>; 129, 208 <245>). 239

As far as the protection of the core area at a subsequent level is concerned, prohibitions regarding the use of inadmissible evidence and data deletion requirements, including documentation requirements to this effect, must be provided for, while screening by an independent body is not always necessary (cf. BVerfGE 129, 208 <249>). Regarding telecommunications surveillance, the legislature can in fact determine that such screening is conditional upon whether and to what extent it is likely that the surveillance measure will also encompass highly private information. In that respect, there is an interrelation with the precautionary measures taken at the data collection level. 240

To that end, the legislature is given considerable leeway to design. […] 241

bb) § 20l sec. 6 BKAG satisfies these requirements for the most part. 242

(1) Substantively, § 20l sec. 6 sentence 1 BKAG stipulates that an assessment with regard to the protection of the core area must be carried out before implementing telecommunications surveillance measures and that such measures may not be taken if there are factual indications suggesting that the measure will only generate insights from the core area of private life. Given that this provision is also subject to a constitutional understanding according to which conversations with highly trusted persons are not already removed from the strict scope of protection if these conversations combine highly personal with everyday matters (cf. BVerfGE 109, 279 <330>), this is not objectionable. In accordance with the Constitution, the Act also stipulates that the measure be discontinued if the surveying persons gain direct knowledge of highly confidential conversations; furthermore, if doubts arise, the Act limits the surveillance measure to automatic recordings, § 20l sec. 6 sentences 2 and 3 BKAG. 243

However, beyond that, the Act also allows automatic recording measures in general, i.e. even in those cases in which such measures might also encompass, in addition to other conversations, conversations that are of relevance with regard to the core area (cf. first half of § 20l sec. 6 sentence 2 BKAG). As far telecommunications surveillance is concerned, this is, nonetheless, still constitutionally acceptable. In that respect, the more stringent requirements applying to the surveillance of private homes (cf. BVerfGE 109, 279 <324>), which are, given their nature, more closely linked to the core area, are not applicable here. Nonetheless, an order to carry out such automatic recording is subject to a strict proportionality test assessing the measure's temporal and factual scope in the individual case. Also, the fact that this provision accepts that measures might cover highly personal information requires effective protective precautions at the level of the analysis and use of the data. 244

(2) Also in this respect, the provision meets the constitutional requirements for the most part. The provision not only provides for the required prohibitions regarding the use of inadmissible evidence and data deletion requirements, but, regarding automatic recordings, also requires prior screening by a court. The fact that this review is limited to automatic recordings and thus to covering cases of doubt does not raise constitutional concerns. Unlike in case of the surveillance of private homes, the independent screening of telecommunications surveillance may be limited to cases of doubt. 245

In contrast, however, the safekeeping period for the deletion protocols set out in § 20l sec. 6 sentence 10 BKAG is too short and thus unconstitutional (see above, C IV 3 d). 246

6. Insofar as it corresponds to § 20l BKAG, § 20m secs. 1 and 3 BKAG suffers from the same constitutional deficiencies and is itself also unconstitutional in this respect. As for the rest, the provision is compatible with the Constitution. 247

a) § 20m secs. 1 and 3 BKAG, which allows the collection of telecommunications traffic data, provides the basis for an interference with the right to secrecy of telecommunications under Art. 10 sec. 1 GG. This right protects not only the actual contents of the communication but also the confidentiality of the specific circumstances of communication events which include in particular whether, when and how often telecommunications traffic occurred or was attempted between whom or between which telecommunications equipment (cf. BVerfGE 67, 157 <172>; 130, 151 <179>; established case-law). 248

An interference with Art. 10 sec. 1 GG by means of the collection of telecommunications traffic data is serious – even if it does not directly cover the contents of the communication (cf. BVerfGE 107, 299 <318 et seq.>; regarding the precautionary storage of such telecommunications traffic data cf. also BVerfGE 125, 260 <318 et seq.>). However, if designed proportionately, it can be justified for the purpose of protecting against terrorism. As with § 20l BKAG, this is, however, not the case in all respects. 249

b) Regarding the constitutional appraisal of the provision, whose conditions for interference essentially correspond to those set out in § 20l secs. 1 and 3 to 5 BKAG, the statements made in that context apply here accordingly. Given that the requirements for investigative and surveillance measures constituting a serious interference, stemming from the overarching principle of proportionality, are not met in this respect (see above, C IV 1 b, 2), the approach taken with regard to the collection of telecommunications traffic data does not differ from that applied in content-related surveillance of telecommunications. 250

Accordingly, § 20m sec. 1 no. 2 BKAG is not compatible with the Constitution, while § 20m sec. 1 nos. 3 and 4 BKAG requires an interpretation in conformity with the Constitution; a statutory obligation to substantiate the reasons underlying the order of the measure is lacking, too (see above, C V 5 b, d). 251

As for the rest, § 20m secs. 1 and 3 BKAG is compatible with the Constitution. […] Also § 20m sec. 3 sentence 2 BKAG, which, in view of ordering measures, provides for a facilitation of the description of the data to be collected, does not raise constitutional concerns; this does not have implications for the fact that § 20m sec. 1 BKAG allows the collection of data only with regard to individual persons. 252

VI.

In several respects, the challenged investigative and surveillance powers are not compatible with the Constitution in terms of the further requirements that they too must meet (see above, C IV 4 to 7). They lack supplementary provisions without which the proportionality of the challenged investigative and surveillance powers is not satisfied. 253

1. It is not objectionable, however, that the Act does not contain an express rule that specifies in detail the prohibition of comprehensive surveillance with a view to the interplay of the different powers (see above, C IV 4). Stemming from the principle of proportionality, the prohibition of comprehensive surveillance serves the purpose of safeguarding, for constitutional reasons, the inalienable core of personality that is rooted in human dignity; within their powers, security authorities must observe this prohibition upon their own initiative (cf. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; established case-law). Insofar, further statutory specifications are not required. […] 254

2. However, the degree of protection of professional groups and other groups of persons whose activities require, for constitutional reasons, that their communication be treated as particularly confidential is not viably designed in all respects. 255

a) Yet with § 20u BKAG, the legislature has created a provision that largely meets the relevant constitutional requirements. In particular it is not objectionable that § 20u sec. 2 BKAG – drafted closely in line with § 160a StPO – does not strictly rule out the surveillance of persons subject to professional confidentiality but rather rules out such surveillance only subject to a weighing of considerations in the individual case, and requires in § 20u sec. 1 BKAG a stricter prohibition of surveillance only with a view to a small group of persons whom the legislature has identified as being in particular need of protection (cf. BVerfGE 129, 208 <258 et seq.>). The weighing of considerations required under § 20u sec. 2 BKAG needs to give appropriate weight to the affected persons' fundamental rights. The weighing is structured in line with the principle of proportionality. In accordance with the second half of § 160a sec. 2 sentence 1 StPO, the Constitution sets down the presumption that the interests of the Federal Criminal Police Office in collecting data generally will not prevail if the measure does not aim to provide protection against a significant danger. 256

b) In that respect, however, the level of protection afforded to the relationship of trust between lawyers and their clients is not compatible with the Constitution. The legislative distinction between defence counsel and other lawyers acting within a lawyer-client relationship does not as such constitute a suitable criterion for differentiating the respective protection level, given that the surveillance measures in question do not pursue the aim of prosecuting criminal offences but of protecting against threats, meaning that criminal defence is in fact not of any relevance here. 257

c) Beyond that, however, violations of fundamental rights resulting from § 20u BKAG are not discernible. In particular, Art. 5 sec. 1 sentence 2 GG does not result in media representatives being entitled to claim stricter protection (cf. BVerfGE 107, 299 <332 and 333.>). Further limits do not stem from Art. 3 sec. 1 GG either. The legislature is permitted to understand the recognition of stricter protection against surveillance measures as an exception for specific situations requiring protection and with regard to which the legislature's discretion is broad. In a judgment of 12 October 2011, the Second Senate ruled that the recognition that clergy or political representatives are in need of special protection compared to other 258

professional groups is sound at least. However, an obligation to also extend this particular level of protection to other groups cannot be derived from that finding (cf. BVerfGE 129, 208 <258 et seq., 263 et seq.>). […]

3. The provisions aiming to guarantee transparency, legal protection, and supervisory control do not satisfy the constitutional requirements in all respects either. 259

a) When construed appropriately, the drafting of obligations to notify as set out in § 20w BKAG is not objectionable. The provision, which is drafted closely in line with § 101 secs. 4 to 6 StPO, satisfies the constitutional requirements (cf. BVerfGE 129, 208 <250 et seq.>). 260

The same applies with regard to the second half of § 20w sec. 2 sentence 1 BKAG, which allows refraining from notification for the purpose of securing the further deployment of an undercover investigator. Unlike the case where the notification of the deployment of undercover investigators for the surveillance of private homes is deferred – for which this purpose is not sufficient (cf. BVerfGE 109, 279 <366 and 367>) –, this exception from the obligation to notify concerns the deployment of an undercover investigator as such. […] 261

The permission to refrain definitely from a notification after a period of at least five years according to § 20w sec. 3 sentence 5 BKAG, is constitutional. In accordance with the current practice of definitively deciding to refrain from a notification as described by Federal Criminal Police Office representatives in the oral hearing, such decisions, when interpreting the provision in conformity with the Basic Law, require that a further use of the data against the affected person be ruled out and the data deleted. 262

b) With regard to the challenged investigative and surveillance powers, the rights to information as well as the possibility of a retrospective judicial review and, where appropriate, compensation are guaranteed in a manner that does not raise constitutional objections. 263

[…] 264-265

c) In contrast, supervisory control requirements are not designed in a constitutionally sufficient manner (see above, C IV 6 d). Indeed, the provisions of the Federal Data Protection Act demand a review by the Federal Data Protection Commissioner who has adequate powers in that respect (cf. BVerfGE 133, 277 <370 para. 215>). However, sufficient statutory requirements of regular mandatory reviews that must take place at certain minimum intervals of approximately two years are lacking (cf. BVerfGE 133, 277 <370 and 371, para. 217>). 266

Comprehensive documentation requirements that allow the full and effective review of the surveillance measures in question are lacking, too (cf. BVerfGE 133, 277 <370, para. 215>). The Act does set out sporadic documentation requirements, such as in § 20k sec. 3 BKAG regarding the access to information technology systems or in § 20w sec. 2 sentence 3 BKAG regarding the deferral of a notification. However, even in those cases that require the documentation of the notification, it remains unclear whether this also includes the reasons for a deferral. In any event, the provisions remain sporadic and fail to adequately ensure a retrospective review of the surveillance measures. While important findings resulting from the data collection are at least documented on the basis of the general rules for file keeping, this is neither set out with sufficient clarity nor statutorily with regard to the data protection law requirements of effective review. This is particularly significant in the area of the protection against threats where the investigation of and protection against threats does not need to be directed at specific individual persons, unlike in the case of criminal investigations in criminal proceedings. Insofar, it is not apparent that there is a guarantee that the collection of data is documented in a transparent manner – also from the perspective of affected parties in potential subsequent criminal proceedings. The fact that the measure requires a judicial order does not alter this finding, given that such an order only gives the permission to carry out the measure but does not indicate whether and to what extent use was made of it. Furthermore, and unlike in the case of criminal proceedings pursuant to § 100b sec. 4 sentence 2 StPO, there is not even a requirement demanding that the ordering court be informed of the results of the investigations. 267

d) Finally, reporting duties vis-à-vis Parliament and the public that are necessary for a proportionate design of the challenged surveillance powers are lacking, too (cf. BVerfGE 133, 277 <372 paras. 221 and 222>). The law neither requires reports indicating the degree in which the powers were made use of and on the grounds of which suspicious circumstances, nor does it require reports providing information as to whether the affected parties were notified of the exercise of such powers and if so to what extent. However, given that the exercise of the powers in question occurs largely without the knowledge of the affected party and the public, such reports are constitutionally required at regular intervals in order to enable a public debate and democratic control (see above, C IV 6 e). 268

4. The provision in § 20v sec. 6 BKAG governing the requirements to delete the collected data also does not satisfy the constitutional requirements in all respects. 269

a) The overall structure of the provision is indeed not objectionable under constitutional law. Data must be deleted after the underlying reason for the data collection is fulfilled (sentence 1). This refers to the constitutional law principle of purpose limitation (see below, D I). Accordingly, with regard to a further use of the data pursuant to § 20v sec. 4 sentence 2 BKAG, refraining from deleting the collected data beyond the specific incident is, when interpreting the provision in conformity with the Constitution, only permissible insofar as the data provides a specific evidentiary basis for further investigations to protect against threats from international terrorism. The deletion must be documented (sentence 2). The deletion may be deferred so as to be available for a possible judicial review; in that case, the data in question needs to be blocked (sentence 4). Procedurally, the provision is to be read in conjunction with § 32 BKAG. In addition to requiring an individual handling of cases, that provision's section 3 also requires periodic reviews of the deletion requirements. 270

Regarding electronic profile searching measures, § 20j sec. 3 BKAG sets out specific deletion requirements which the provision specifies in a manner that does not raise constitutional objections. 271

b) In contrast, however, the very brief safekeeping period for the deletion of the "files" in § 20v sec. 6 sentence 3 BKAG, with which the Act governs the deletion of the deletion protocols, is not compatible with constitutional requirements. Deletion protocols serve the purpose of enabling the tracing back and review of the deletion. Thus, the safekeeping period must be calculated so as to ensure that the logs still exist after the persons concerned have been notified, and are still available for the next pending periodic review by the Federal Data Protection Commissioner (cf. in this respect also BVerfGE 100, 313 <400>). 272

The same applies accordingly to the safekeeping period set out in § 20j sec. 3 sentence 3 BKAG. 273

c) Furthermore, § 20v sec. 6 sentence 5 BKAG is unconstitutional. The provision gives permission to refrain from deleting the data once it has served its purpose on grounds that the data is needed for law enforcement purposes or – pursuant to the standards set out in § 8 BKAG – for the prevention of crimes or as a precaution for the future prosecution of a criminal offence of considerable significance. Thus the provision allows the storage of data with a view to using it for new purposes that are, however, only circumscribed in general terms; the Act does not provide a legal authorisation to that end for such generally circumscribed purposes and in fact could not provide a legal authorisation in such broadness. 274

D.

Insofar as the constitutional complaints are directed against the powers to further use the data and the powers to transfer data to domestic authorities and authorities in third countries, the complaints are also well-founded in several respects. 275

I.

The requirements for the further use and transfer of data collected by the state follow the principles of purpose limitation and change in purpose (cf. BVerfGE 65, 1 <51, 62>; 100, 313 <360 and 361, 389 and 390>; 109, 279 <375 et seq.>; 110, 33 <73>; 120, 351 <368 and 369>; 125, 260 <333>; 130, 1 <33 and 276

34>; 133, 277 <372 et seq. paras. 225 and 226>; established case-law).

If the legislature also permits the use of data beyond the specific incident and beyond the reason justifying the data collection it must establish a distinct legal basis to that end (cf. only BVerfGE 109, 279 <375 and 376>; 120, 351 <369>; 130, 1 <33>; established case-law). Insofar, the legislature may, on the one hand, provide for a further use of the data in the context of the purposes determining the data collection. Provided that the legislature ensures that the further use of data satisfies the specific constitutional requirements of the principle of purpose limitation, such an approach is generally constitutionally permissible (1.). On the other hand, the legislature may also allow a change in purpose. As an authorisation for the use of data for new purposes this is, however, subject to specific constitutional requirements (2.). 277

1. The legislature may allow a use of the data beyond the specific procedure of the data collection as a further use in the context of the original purposes of the data. Insofar, the legislature may invoke the justification underlying the data collection and is thus not subject to the constitutional requirements applied to a change in purpose. 278

a) The permissible scope of such uses depends on the authorisation for the data collection. The respective legal basis for interferences determines the competent authority as well as the purpose of and conditions for data collection and thus defines the permissible scope of use. Accordingly, the principle of purpose limitation that applies with regard to information obtained on the basis of the authorisation is not a restriction to certain abstractly defined functions of the authorities but is determined in accordance with the scope of the collection purpose stipulated in the relevant legal basis for the respective case of data collection. For that reason, further use of the data within the scope of the originally determined purpose is only permissible insofar as it involves the same authority acting within the same assignment of tasks and for the protection of the same legal interests as were determinant for the data collection. If this specific permission to collect data is restricted to collection for the purpose of protecting certain legal interests or preventing certain criminal offences, this limits both its immediate and its further use even by the same authority insofar as there is no other legal basis allowing a further use in the context of a permissible change in purpose. 279

b) Generally, the relevant intervention thresholds required for the collection of data, such as the traditional thresholds requiring a sufficiently specific risk situation in the context of the protection against threats or a sufficiently strong suspicion in the context of criminal prosecution, do not belong to the purpose limitations that the same authority must reconsider for each and every further use of data. The requirement of there being a sufficiently specific risk situation or a qualified suspicion determines the grounds that may prompt the permission to collect data. Such requirements do not, however, determine the permissible purposes for which the authority may then use the data. 280

For that reason, the principle that data must be used in accordance with its original collection purpose is not automatically contradicted if the further use of such data is permitted as a mere evidentiary basis for further investigations (*Spurenansatz*) when performing the same task, irrespective too of further legal requirements. Insofar, the authority may use the findings thus obtained – either alone or in combination with all other available information – as a simple starting point for further investigations to protect the same legal interests within the same assignment of tasks. This takes into account that it is not possible to reduce the generation of knowledge – and not least when aiming to understand terrorist structures – to a mere sum of separated and individual data which one could reveal or suppress in line with legal criteria. Within the described limits, this is recognised by the legal order. […] 281

Observance of the principle of purpose limitation depends on whether the authority that is empowered to collect data uses it while acting within the same assignment of tasks for the protection of the same legal interests and the prosecution or prevention of the same criminal offences as is determined in the relevant data collection provision. These requirements are necessary but generally also sufficient to legitimise a further use of the data within the scope of the principle of purpose limitation. 282

However, with regard to data obtained by means of the surveillance of private homes and remote searches, the principle of purpose limitation is broader in scope: here, any further use of the data only correlates with the purpose if it is also necessary in accordance with the collection requirements of a corresponding imminent danger (cf. BVerfGE 109, 279 <377, 379>) or a specific impending danger (cf. BVerfGE 120, 274 <326, 328 and 329>). The extraordinary weight of the interference resulting from such data collection is also reflected in a particularly narrow limitation of any further use of the obtained data to the requirements and thus to the purposes of the data collection.These findings may not be used as a mere evidentiary basis for further investigations irrespective of an imminent or specific impending danger. 283

2. The legislature may also allow for a further use of data for other purposes than those determining the original data collection (change in purpose). In that case, however, the legislature must ensure that the weight of the interference resulting from the data collection is also taken into consideration with regard to the new use of data (cf. BVerfGE 100, 313 <389 and 390>; 109, 279 <377>; 120, 351 <369>; 130, 1 <33 and 34>; 133, 277 <372 and 373 para. 225>). 284

a) The authorisation to use data for new purposes constitutes a new interference with the fundamental right with which the data collection interfered (cf. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 and 69>; 125, 260 <312 and 313, 333>; 133, 277 <372 para. 225>; cf. also ECtHR, Weber and Saravia v. Germany, judgment of 29 June 2006, no. 54934/00, para. 79, NJW 2007, p. 1433 <1434>, on Art. 8 ECHR). For that reason, changes in purpose need to be measured against those fundamental rights that were relevant for the data collection. This applies to any type of data use for purposes differing from those for which the data was originally collected, irrespective of whether the use pursues evidential purposes or constitutes a mere evidentiary basis for further investigations (cf. BVerfGE 109, 279 <377>). 285

b) In that respect, an authorisation to change the purpose is subject to the principle of proportionality. The weight attached to such a provision when weighing considerations corresponds to the weight of the interference resulting from the data collection. Information obtained by measures constituting a serious interference may only be used for particularly weighty reasons (cf. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277 <372 and 373 para. 225>, with further references). 286

aa) Regarding the standards applied to the proportionality test, the former case-law of the Federal Constitutional Court reviewed whether the changed use was “incompatible” with the original purpose (cf. BVerfGE 65, 1, <62>; 100, 313 <360, 389>; 109, 279 <376 and 377>; 110, 33 <69>; 120, 351 <369>; 130, 1 <33>). Meanwhile, this approach has been specified and replaced by the criterion of a hypothetical re-collection of data (*hypothetische Datenneuerhebung*). Accordingly, as far as data that results from particularly intrusive surveillance and investigative measures is concerned, such as the data at issue in these proceedings, it is necessary to determine whether it would be permissible, by constitutional standards, to also collect the relevant data for the changed purpose with comparably weighty means (cf. BVerfGE 125, 260 <333>; 133, 277 <373 and 374 paras. 225 and 226>; in substantive terms, this specification is not new cf. already BVerfGE 100, 313 <389 and 390> and is referred to as a “hypothetical substitute interference” in BVerfGE 130, 1 <34>). However, the criterion of a hypothetical re-collection of data is not applied in a rigid systematic manner and does not rule out the possibility that further aspects may be taken into consideration (cf. BVerfGE 133, 277 <374 para. 226>). Thus the fact that the authority receiving the data is not – unlike the authority that permissibly collected the data and from which the data emanates – empowered to collect certain data itself due to its assignment of tasks does not bar, as a matter of principle, the exchange of data between these authorities (cf. BVerfGE 100, 313 <390>). Furthermore, when establishing data transfer provisions, considerations such as simplification and practicability can justify the fact that not all individual requirements that must be met for the collection of data will also apply, with the same level of detail, to the transfer of data. This, however, does not affect the requirement that the new use must be of equal weight. 287

bb) However, for that reason a requirement for a change in purpose is that the new use of the data must serve the protection of legal interests or aim to detect criminal offences of such a weight that would, by constitutional standards, justify collecting them again with comparably weighty means (cf. BVerfGE 100, 288

313 <389 and 390>; 109, 279 <377>; 110, 33 <73>; 120, 351 <369>; 130, 1 <34>).

In contrast, the requirements for a change in purpose are not always identical to the requirements for a data collection with regard to the necessary degree of specificity of the risk situation or of the suspicion that a crime has been committed. With a view to proportionality considerations, the relevant requirements primarily only establish the direct grounds for the data collection as such but not also those for the further use of the collected data. An authorisation to use data for other purposes constitutes an interference that requires a new justification. For that reason, such an authorisation also requires its own, sufficiently specific grounds. Under constitutional standards, it is thus necessary but generally also sufficient that the data – either as such or in combination with the authority's additionally available information – results in a specific evidentiary basis for further investigations. 289

With regard to the use of data by security authorities, the legislature may thus generally allow for a change in purpose of data if it concerns information that results, in individual cases, in a specific evidentiary basis for further investigations investigating comparably serious criminal offences or providing protection against threats that, at least in the medium term, threaten comparably weighty legal interests as those with regard to whose protection the respective data collection is permissible. 290

The same, however, does not apply with regard to information obtained through the surveillance of private homes or access to information technology systems. Considering the significant weight of the interference reflected in these measures, each and every new use of data is subject to the same justification requirements as the data collection itself in that the new use also requires imminent danger (cf. BVerfGE 109, 279 <377, 379>) or a sufficiently specific impending danger (see above, C IV 1 b). 291

cc) These requirements for the permissibility of a change in purpose reflect a specifying consolidation of a long line of jurisprudence developed by both Senates of the Federal Constitutional Court (cf. BVerfGE 65, 1 <45 and 46, 61 and 62>; 100, 313 <389 and 390>; 109, 279 <377>; 110, 33 <68 and 69, 73>; 120, 351 <369>; 125, 260 <333>; 130, 1 <33 and 34>; 133, 277 <372 and 373 para. 225>). It does not constitute an intensification of the standards but carefully delimits them in that it does not apply the criterion of a hypothetical re-collection of the data in a strict manner (cf. already BVerfGE 133, 277 <374 para. 226>) but instead partially revokes former requirements with regard to the interference thresholds that determine the required temporal proximity of the risk situation (cf. in particular BVerfGE 100, 313 <394>; 109, 279 <377>). Also giving up the requirement of a protection of comparably weighty legal interests – as suggested in one of the separate opinions – would mean that the limits of the principle of purpose limitation as a core element of constitutional data protection (cf. BVerfGE 65, 1 <45 and 46, 61 and 62>) would practically be rendered obsolete with regard to security law – in particular if the requirement of a specific evidentiary basis for further investigations is at the same time held to be too strict (or at most these limits would be limited rudimentarily to data stemming from the surveillance of private homes or remote searches). 292

II.

In light of the abovementioned standards, § 20v sec. 4 sentence 2 BKAG, which sets out how the Federal Criminal Police Office may use data it collected itself, does not satisfy constitutional requirements. The provision is unconstitutional. 293

1. The use of data as set out in § 20v sec. 4 sentence 2 no. 1 BKAG solely with regard to carrying out tasks to protect against threats from international terrorism is generally compatible with constitutional requirements; however, the provision lacks a sufficient limitation for data obtained through the surveillance of private homes and remote searches. 294

a) Generally, the provision does not give rise to effective constitutional concerns. 295

aa) The provision gives the Federal Criminal Police Office the permission to use data it collected itself for the purpose of protecting against international terrorism in the performance of its duties pursuant to § 4a sec. 1 sentence 1 BKAG. With that, the provision first – as an inherent consequence of authorising the collection of data – enables the use of the data in accordance with the specific purpose for which it was collected. Furthermore, however, it also enables a use of the data that goes beyond the respective investigation procedure. Due to the reference to § 4a sec. 1 sentence 1 BKAG, this further use of the data is limited to the protection against international terrorism. When applying a factually appropriate understanding of this reference, it also determines that the data may only be used to prevent those qualified criminal offences mentioned in § 4a sec. 1 sentence 2 BKAG and thus only for the protection of those high-ranking legal interests regarding which the data collection powers of subsection 3a – including the particularly intrusive surveillance powers in §§ 20g et seq. BKAG – may be deployed for protection purposes. 296

(1) The reference to § 4a sec. 1 sentence 1 BKAG, however, raises doubts as to its meaning. These can be overcome by way of interpretation so that the provision does not fail to meet specificity standards. It is not clear how § 4a sec. 1 sentence 1 and 2 BKAG are to be delimited: in assigning the task of providing protection against dangers, sentence 1 is aligned with the wording of Art. 73 sec. 1 no. 9a GG which also covers the prevention of criminal offences (see above, C I 1); sentence 2, however, explicitly distinguishes between the prevention of criminal offences and the protection against dangers. However, due to its nature as a provision setting out duties for the protection against dangers, § 4a sec. 1 sentence 1 BKAG also includes investigations in advance of specific dangers, and the reference in § 20v sec. 4 sentence 2 no. 1 BKAG is thus, essentially, sufficiently open to interpretation after all; the provision aims to allow the use of data in general, and, if necessary, also as a mere evidentiary basis for further investigations, for the purpose of providing protection against threats from international terrorism. 297

In addition, the provision is not too unspecific insofar as § 4a sec. 1 BKAG only generally refers to “threats from international terrorism”. Even though § 20v sec. 4 sentence 2 no. 1 BKAG only refers to sentence 1 of the provision, the further specification of the dangers listed therein requires resorting to the detailed definition in sentence 2, which conclusively enumerates and further specifies certain criminal offences. The fact that the criminal offences enumerated there with regard to the prevention of criminal offences are also decisive for the protection against threats under sentence 1 also conforms to the systematics of the Act as such (cf. e.g. § 20a sec. 2 BKAG). 298

(2) Given that § 20v sec. 4 sentence 2 no. 1 BKAG allows the use of data only to protect against threats from terrorist offences within the meaning of § 4a sec. 1 sentence 2 BKAG, this also ensures that this use is only permitted for the protection of those legal interests in regard to which the data collection powers may also be exercised. The same applies to data obtained by particularly intrusive surveillance measures, which are only justified for the protection of particularly high-ranking legal interests. 299

Nearly all criminal offences enumerated in § 4a sec. 1 sentence 2 BKAG in conjunction with § 129a secs. 1 and 2 StGB concern crimes that are directly directed against life or limb or – for example, as crimes endangering the general public – that draw their wrongful nature from threats thereto, or concern property of substantial value of value the preservation of which as essential infrastructure is in the public interest. Insofar as this is not necessarily the case with some individual crimes enumerated in § 129a StGB, it needs to be taken into account that § 4a sec. 1 sentences 1 and 2 BKAG determines that the prevention of such criminal offences only falls within the Federal Criminal Police Office’s remit if the offences have a terrorist dimension that is statutorily defined in greater detail. Thus, the factually appropriate understanding of the provision results in the finding that information obtained through individual investigative powers must, also when resorted to for a further use pursuant to § 20v sec. 4 sentence 2 no. 1 BKAG, always serve to protect those legal interests for whose protection the collection of data was already justified, even in the case of more intrusive measures. 300

bb) Generally, it is not objectionable either that § 20v sec. 4 sentence 2 no. 1 BKAG allows the further use of data in general terms and thus also as a mere evidentiary basis for further investigations 301

irrespective of specific threats or specific evidentiary bases. Insofar as the use does not concern data stemming from the surveillance of private homes or remote searches (see below, D II 1 b), it it still within the scope of the purpose limitation. […] This, however, does not affect the requirement to delete the recorded data after achieving the purpose of the data collection (see above, C VI 4 a).

b) § 20v sec. 4 sentence 2 no. 1 BKAG is, however, disproportionately broad insofar as it covers all data indiscriminately and thus also covers the further use of data stemming from the surveillance of private homes and remote searches. Accordingly, the provision allows the further use of data irrespective of whether there is an imminent danger (cf. BVerfGE 109, 279 <377, 379>) or a risk situation that is sufficiently specific in the individual case (see above, C IV 1 b; D I 2 b bb). This is incompatible with the constitutional prohibition of excessiveness. As far as information that stems from such particularly intrusive surveillance measures is concerned, any use that goes beyond the original investigations requires that all conditions for interference be met again each time and in the same way as would be necessary on constitutional grounds in case of a re-collection of data (see above, D I 1 b). 302

2. § 20v sec. 4 sentence 2 no. 2 BKAG, on the use of data for the protection of witnesses and other persons, is also incompatible with constitutional requirements. Due to its lack of specificity alone, the unrestricted and general reference to the duties of the Federal Criminal Police Office under § 5 and § 6 BKAG does not satisfy the standards developed above. 303

III.

Various rules within § 20v sec. 5 BKAG, which governs the transfer of data to other authorities, do not satisfy the constitutional requirements. 304

1. § 20v sec. 5 BKAG provides various legal bases for the transfer of data, collected for the purpose of preventing terrorist threats, to other authorities. The relevant rules constitute authorisations with which the legislature allows a change in purpose of the use of data in individual cases and with regard to specific grounds. In that way, the legislature allows the use of data by other authorities, which – in accordance with the image of a double door – themselves must also be authorised to retrieve and use this data (cf. BVerfGE 130, 151 <184>). Thus, the provision provides for interferences with fundamental rights, each of which must be measured against those fundamental rights that were interfered with by the collection of the transferred data (cf. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 and 69>; 125, 260 <312 and 313, 333>; 133, 277 <372 para. 225>; cf. also ECtHR, Weber and Saravia v. Germany, judgment of 29 June 2006, no. 54934/00, § 79, NJW 2007, p. 1433 <1434>, on Art. 8 ECHR). 305

2. § 20v sec. 5 BKAG does not violate the requirements of the principle of specificity. This also applies insofar as the provision comprehensively allows a transfer of data to “other public entities”. The specific understanding of this phrasing, i.e. identifying which entities are meant, depends on the respective transfer purposes which further specify the different transfer powers. It is thus possible to determine the potential addressees of a transfer with sufficient specificity on the basis of the competence provisions. 306

3. Yet the transfer powers are unconstitutional insofar as their requirements fail to satisfy the standards developed above with regard to the criterion of a hypothetical re-collection of data (see above, D I 2 b). 307

a) § 20v sec. 5 sentence 1 no. 1 BKAG, however, does not raise constitutional concerns. The transfer of data for the purpose of mutual understanding and coordination does not itself implicate a change in purpose. It aims to coordinate the protection against threats in a manner that § 4a sec. 2 BKAG always requires for the Federal Criminal Police Office to exercise its functions, and is thus necessarily included in the data collection provision. This also justifies the broadness of the provision that does not provide restrictions to the transfer of data. Coordination is only provided for with regard to measures that are based on a lawful use of data; for that reason, it need not be feared that the purpose limitation of information stemming from the surveillance of private homes or remote searches, and which may be used only if there is a sufficiently specific risk situation, is undermined. 308

In functional terms, however, the provision is to be construed narrowly. It only allows the transfer of information for the purpose of coordinating the exercise of the tasks of federal and *Laender* authorities, respectively. Under this provision, the use of data is limited to such internal coordination. If, in contrast, the authority receiving the data should be allowed to also use also for operational purposes, the transfer is subject to § 20v sec. 5 sentence 1 nos. 2 et seq. BKAG. 309

b) § 20v sec. 5 sentence 1 no. 2 BKAG governs the transfer of data for the purpose of protecting against threats. For the most part, it satisfies constitutional requirements. However, the provision is disproportionate insofar as it generally already allows a transfer of data for the prevention of certain criminal offences. 310

aa) § 20v sec. 5 sentence 1 no. 2 BKAG allows a transfer of data stemming from measures taken pursuant to §§ 20h, 20k or 20l BKAG for the purpose of protecting against an imminent threat to public security. With this threshold, which is directly deduced from Art. 13 sec. 4 GG, the legislature, with regard to a change in purpose, conforms to the requirements for a hypothetical re-collection of data; also, a transfer of information from particularly intrusive measures, including the surveillance of private homes and remote searches, is justified. While it is generally the duty of the legislature to specify the legal interests to be protected in the context of conditions for interference and to thus also flesh out the concept of public security which, while being enshrined in Art. 13 sec. 4 GG, is described only in general terms (cf. accordingly for Art. 14 sec. 3 GG BVerfGE 134, 242 <294 para. 177>), here such specifications can be deduced from the regulatory context. Upon a reasonable interpretation, the concept of an imminent threat to public security must be held to mean a threat to the particularly high-ranking legal interests enumerated in §§ 20h, 20k and 20l BKAG (cf. in this respect also BVerfGE 109, 279 <379>). 311

bb) It is not objectionable either that the transfer of data collected by means of other measures only requires a significant danger to public security. It is, first, not objectionable with regard to data obtained by means of low-threshold interferences (cf. for example §§ 20c et seq. or §§ 20q et seq. BKAG). The transfer of such data is, to be permissible, generally subject to less restrictive requirements. Furthermore, the provision is also constitutional with regard to data from intrusive measures such as those adopted pursuant to §§ 20g, 20j or 20m BKAG. Also here, the public security concept is not to be interpreted as being as comprehensive as in the sense of the general clause of police law that relates to the inviolability of the legal order […]. Instead it is given shape by the term “significant” danger. In accordance with the respective interpretation under general security law, this requires that there be a danger to an important legal interest; this includes life, limb, freedom or the existence of the state in particular […]. An interpretation of the provision based on the Constitution must result in the conclusion that a precondition for the transfer of data from particularly intrusive measures is the protection of sufficiently weighty legal interests. 312

cc) However, § 20v sec. 5 sentence 1 no. 2 BKAG is disproportionately broad and thus unconstitutional insofar as it generally also allows a transfer of data for the purpose of preventing criminal offences enumerated in § 129a secs. 1 and 2 StGB. Indeed, these all constitute particularly serious criminal offences. However, given that the Act allows the transfer in general terms for the purpose of preventing such criminal offences, it fails to provide for a restricting specification of the transfer in line with the particular grounds prompting the transfer; thus information can already be transferred as a mere evidentiary basis for further investigations even if it only has potential informative value – and even if it was obtained by means of intrusive measures. In light of the standards developed above, this does not satisfy constitutional requirements (see above, D I 2 b bb). A transfer of data from intrusive surveillance measures to other security authorities constitutes a change in purpose and is only permissible if it involves at least a specific evidentiary basis for further investigations for the detection of equivalent criminal offences. The provision, however, fails to ensure that this requirement is adhered to. 313

c) § 20v sec. 5 sentence 1 no. 3 BKAG, which governs the transfer of data for criminal prosecution purposes, is not compatible with the Constitution either. 314

aa) The provision is disproportionate insofar as its first case group for a transfer of data generally refers to the standards set out in the Code of Criminal Procedure regarding a request for information and thus also refers to data from surveillance measures that are not specifically mentioned in no. 3 sentence 2 but are, nonetheless, intrusive surveillance measures such as those taken pursuant to §§ 20g, 20j or 20m BKAG. With its reference to the Code of Criminal Procedure, the provision refers to § 161 secs. 1 and 2 StPO in particular. This provision, however, does not ensure the constitutionally required limitation of the transfer of data. In particular, it does not follow from the provision that data may only be used to prosecute those criminal offences regarding which it would have been permissible to collect the data with the appropriate means (see above, D I 2 b). In fact, § 161 sec. 1 StPO provides an information obligation and thus an obligation to transfer data with respect to every type of criminal act. The restrictions contained in § 161 sec. 2 StPO only refer to the use of data in criminal proceedings for evidentiary purposes. Against that background, the stipulated restrictions do not rule out the possibility that the data be used as a mere evidentiary basis for further investigations for the investigation of any criminal offence, including minor crimes […]. This, however, fails to ensure the constitutionally required restriction of a change in use of data to the protection of equally important legal interests. Moreover, the provision fails to guarantee that only data actually indicating that there is a specific evidentiary basis for further investigations in the crimes in question may be transferred. 315

bb) The provision is also disproportionate insofar as its sentence 2 stipulates distinct requirements for the use of data from measures taken pursuant to §§ 20h, 20k and 20l BKAG. The legislature allows their transfer for the purpose of enforcing crimes that are subject to a maximum term of imprisonment of more than five years (§ 20v sec. 5 sentence 1 no. 3, 2nd sentence thereof BKAG). Regarding data obtained through measures carried out pursuant to §§ 20k and 20l BKAG, this constitutes a limitation of the general reference to provisions of the Code of Criminal Procedure and thus to § 161 sec. 1, sec. 2 sentence 1 StPO. In contrast, as far as data stemming from the surveillance of private homes is concerned, it constitutes an expansion, given that a change in use of this data is construed more narrowly in § 161 sec. 2 sentence 2, § 100d sec. 5 no. 3 StPO. Irrespectively, however, this threshold does not satisfy the standards developed with regard to the criterion of a hypothetical re-collection of data. Regarding the surveillance of private homes, the Federal Constitutional Court has explicitly held that a maximum term of imprisonment of more than five years does not constitute a sufficient threshold for ordering such a measure and this also applies to any further use of the data, including its use as a mere evidentiary basis for further investigations (cf. BVerfGE 109, 279 <347 and 348, 377>). The same applies to access to information technology systems, which is an equally significant interference and thus subject to the same requirements. While the requirements for the surveillance of telecommunications are indeed less strict, the collection of data and, accordingly, the power to transfer, which constitutes a change in purpose, at least require that there be a focus on serious criminal offences (cf. BVerfGE 125, 260 <328 and 329>; 129, 208 <243>). For that reason, it is disproportionate that § 20v sec. 5 sentence 1 no. 3, 2nd sentence thereof BKAG states that criminal offences subject to a maximum term of imprisonment of more than five years are sufficient as this also includes crimes of medium severity and possibly also volume crime offences such as simple theft, public slander or simple bodily harm. 316

Furthermore, it is constitutionally objectionable that data stemming from the visual surveillance of private homes is not barred from being transferred to law enforcement authorities. With regard to law enforcement, Art. 13 sec. 3 GG only allows the acoustic surveillance of private homes. This may not be undermined by a transfer of data obtained through a preventatively ordered visual surveillance of private homes. 317

cc) While the transfer of data from particularly intrusive surveillance measures is subject to qualified requirements, the transfer of data obtained by means of low-threshold interferences (cf. for example §§ 20b et seq., §§ 20q et seq. BKAG) is constitutionally permissible on a wider scale. To that end, the 318

requirements set out in § 20v sec. 5 sentence 1 no. 3 BKAG can provide a viable basis. However, in this respect the legislature must distinguish between the different types of data. In its current version, the provision is too broad in that is does not distinguish between different data, and it is thus disproportionate.

d) Also § 20v sec. 5 sentence 3 no. 1 BKAG, which allows the transfer of data to offices for the protection of the Constitution (*Verfassungsschutzbehörden*) and the Military Counter Intelligence Agency (*Militärischer Abschirmdienst*), is incompatible with constitutional requirements. 319

The provision, which applies to all data except that obtained through the surveillance of private homes (cf. § 20v sec. 5 sentence 5 BKAG), allows the transfer of data to the abovementioned authorities provided that there are factual indications suggesting that the data is necessary for the gathering and analysis of information on endeavours falling within the remit of the offices for the protection of the Constitution or the Military Counter Intelligence Agency. For that reason, it does not satisfy the standards of a hypothetical re-collection of data, which is, however, decisive for the transfer of data for a changed purpose (see above, D I 2 b). Indeed, the transfer of data generally pursues the objective of protecting particularly weighty legal interests in that it references the duties of the offices for the protection of the Constitution and the Military Counter Intelligence Agency. Furthermore, with regard to § 8 of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Bundesverfassungsschutzgesetz* – BVerfSchG), which is decisive for a hypothetical re-collection of data, the transfer of certain data, such as that obtained through measures taken pursuant to § 20g BKAG […], can be justified to a relatively broad extent. Yet a provision that allows the transfer of essentially any data for the purpose of supporting the exercise of tasks without determining specific interference thresholds to that end is disproportionately broad. Indeed, the criterion of a hypothetical re-collection of data does not generally require that a specific risk situation, which is required for the collection of data – and which is generally also required for data collection by the offices for the protection of the Constitution, irrespective of the fact that their mandate is essentially limited to activities in the preliminary stages of a threat (cf. BVerfGE 100, 313 <383 and 384>; 120, 274 <329 and 330>; 130, 151 <205 and 206>) – also always be a precondition for each and every case of data transfer (see above, D I 2 b bb). However, for constitutional reasons, it is imperative that the transfer of data be limited to data which, from the perspective of the Federal Criminal Police Office, not only constitutes a specific evidentiary basis for further investigations in criminal offences or dangers to high-ranking legal interests but also, at the same time, reveals specific insights on the endangerment of such legal interests (cf. on the transfer of data from intelligence services to the Federal Criminal Police Office BVerfGE 133, 277 <329 para. 123>) that are relevant for assessment of a situation in accordance with the duties of the offices for the protection of the Constitution. Regarding the transfer of data stemming from remote searches, it is furthermore necessary – like in the case of data stemming from the surveillance of private homes which the legislature has already made specific provision for in this respect – that the interference threshold for the data collection as such is reached, namely a specific impending danger (cf. BVerfGE 120, 274 <326, 328 and 329>). 320

e) Accordingly, § 20v sec. 5 sentence 4 BKAG, too, does not satisfy the constitutional requirements. The provision allows a transfer of data to the Federal Intelligence Service (*Bundesnachrichtendienst*) subject to standards equivalent to those set out in § 20v sec. 5 sentence 3 no. 1 BKAG. The differences in wording do not – considering, too, the legislative reasons of the Act (cf. BTDrucks 16/9588, p. 34) – have an obvious substantive meaning and cannot, at any rate, alter the appraisal in terms of constitutional law. The constitutional deficiencies of § 20v sec. 5 sentence 3 no. 1 BKAG also arise with regard to this provision. 321

4. Finally, all transfer powers lack overarching statutory provisions that ensure sufficient supervisory control. The data collection requirements calling for the substantive documentation and effective review by the Federal Data Protection Commissioner apply here, too (cf. above, C IV 6 d). 322

IV.

In part, § 14 sec. 1 sentence 1 nos. 1 and 3, sentence 2 BKAG, which governs the transfer of data to public authorities of third countries – insofar as § 14a BKAG, which applies to transfers of data to Member States of the European Union, a rule that is not under scrutiny here, is not applicable –, also does not satisfy the constitutional requirements. 323

1. The transfer of personal data to public authorities of third countries is, like the transfer of data to domestic authorities, a change in purpose. Insofar, in accordance with general standards, this change in purpose is to be assessed in light of the relevant fundamental rights with which the data collection interfered (see above, D I 2 a). However, with a view to the due respect owed to foreign legal orders, the transfer of data to third countries is subject to its own constitutional requirements. 324

a) The result of a transfer of data to third countries is that, after the transfer, the guarantees of the Basic Law can no longer be applied as such and the standards prevailing in the respective receiving country apply instead. This does not, however, generally prevent a transfer to third countries. With its Preamble, Art. 1 sec. 2, Art. 9 sec. 2, Art. 16 sec. 2, Arts. 23 to 26 and Art. 59 sec. 2 GG, the Basic Law links the Federal Republic of Germany to the international community and has programmatically aligned the German state authority towards international cooperation (cf. BVerfGE 63, 343 <370>; 111, 307 <318 and 319>; 112, 1 <25, 27>). This includes dealing with other countries even if their legal order and judicial conception does not fully conform to the German domestic conception (cf. BVerfGE 31, 58 <75 et seq.>; 63, 343 <366>; 91, 335 <340, 343 et seq.>; 108, 238 <247 and 248). Such an exchange of data also aims to maintain intergovernmental relations in mutual interests and the Federal Government's freedom of action in the area of foreign policy (cf. BVerfGE 108, 129 <137>). 325

As a starting point, the German state authority, when deciding on the transfer of personal data to third countries, remains bound by the fundamental rights (Art. 1 sec. 3 GG); the foreign state authority is only committed to its own legal obligations. 326

Insofar, limits to the transfer of data emerge, on the one hand, in view of the preservation of data protection guarantees. The limits in the Basic Law on the domestic collection and processing of data may not be undermined in their substance by an exchange of data between security authorities. The legislature must thus ensure that this protection of fundamental rights is not eroded through the transfer of data collected by German authorities to third countries and to international organisations, just as it must not be eroded by the receipt and use of data from foreign authorities that was obtained in violation of human rights. 327

On the other hand, limits to the transfer of data arise with regard to the use of the data by the receiving state if violations of human rights are to be feared. In any event, the transfer of data to third countries is imperatively barred if violations of the fundamental rule-of-law principles are to be feared (cf. BVerfGE 108, 129 <136 and 137>). Under no circumstances may the state be complicit in violations of human dignity (cf. BVerfG, Order of the Second Senate of 15 December 2015 – 2 BvR 2735/14 – para. 62, with further references). 328

b) Accordingly, the transfer of data to third countries presupposes a restriction to sufficiently weighty purposes for which the data may be transferred and used (aa), as well as the ascertainment that the data will be handled in the third country in acceptable conformity with rule of law standards (bb). Apart from that, the guarantee of effective domestic oversight is required here, too (cc). The requirements are to be ensured through specific and clear foundations in German law (dd). 329

aa) As far as the requirements for the purpose of the transfer and use of the data are concerned, the constitutional criteria for a change in purpose, being the relevant standards under the German legal order, apply (see above, D I 2). A transfer is thus permissible insofar as it would be permissible to collect the transferred data with comparably weighty means also for the purpose of the transfer (criterion of a hypothetical re-collection of data). Thus, the transfer must pursue the aim of detecting comparably weighty criminal offences or the protection of comparably weighty legal interests as were relevant for the original data collection. As a rule, however, the transfer is not subject to the requirement that there be a specific 330

risk situation or suspicion of a criminal offence; it suffices that the transferred information or the request by the receiving state show that there is, in the specific case, an evidentiary basis for further investigations for the purpose of detecting such criminal offences or protecting against impending dangers to such legal interests and threatening these at least in the medium term. Insofar, the requirements for the transfer of data stemming from the surveillance of private homes and remote searches are stricter in that this requires that interference thresholds relevant for the data collection are fully complied with (see above, D I 2 b bb; cf. also BVerfGE 109, 279 <377, 379>; 120, 274 <329 et seq.>).

With regard to the resulting necessity of appraising the use of data by the receiving country, which is necessary in particular in the case of a transfer request by a third country, sufficient weight must be attached to the autonomy of the respective other legal order. As far as the question of equal weight of the respective purpose of use is concerned, it needs to be considered in this respect that the German legal order faces another legal order whose parameters, categories and assessments are not identical to those reflected in the German legal order and Basic Law and do not have to be identical. The fact that purpose limitations of the German legal order are insofar not identically reflected in the foreign legal order in the same detail does not bar a data transfer from the outset. When transferring the data, the receiving authorities must be notified clearly and expressly of limitations of use. 331

bb) Furthermore, the transfer of personal data to third countries presupposes that the data will be handled in the third country in acceptable conformity with human rights and data protection standards (1), and requires an according ascertainment by the German state to that end (2). 332

(1) A transfer of data to third countries requires that the data will be handled in the third country in sufficient conformity with rule-of-law standards. 333

(a) In terms of the requirements for the handling of the data in light of data protection standards it is, however, not necessary that the receiving country has enacted rules for the processing of personal data that are comparable to the rules applicable under the German legal order, or that the receiving country provide the same level of protection as the Basic Law. In fact, the Basic Law recognises the autonomy and diversity of legal orders and generally respects them, also in the context of the exchange of data. Parameters and assessments do not need to conform to those of the German legal order or the German Basic Law. 334

However, the transfer of personal data to third countries is only permissible if the handling of the transferred data in these countries does not undermine the human rights protection of personal data. This is not to say that the third country's legal order must guarantee institutional and procedural precautions in line with the German approach; in particular, it is not necessary that there be the same formal and institutional safeguards as required under data protection laws applicable to German authorities (see above, C IV 6). In this sense, it is necessary that an appropriate and substantive level of data protection be guaranteed with regard to the handling of the transferred data by the receiving state (cf. similarly ECJ, Judgment of 6 October 2015 – C-362/14 –, Schrems/Digital Rights Ireland, NJW 2015, p. 3151 <3155>, para. 73; cf. also Art. 8 ECHR; on this ECtHR, [GC], Roman Zakharov v. Russia, no. 47143/06, Judgment of 4.12.2015, §§ 227 et seq.; Art. 17 sec. 1 sentence 1 of the International Covenant on Civil and Political Rights (ICCPR) of 16 December 1966, BGBl. 1973 II p. 1534, UNTS 999, p. 171; Art. 12 of the Universal Declaration of Human Rights (UDHR) of 10 December 1948, General Assembly Res. 217 A III, GAOR III, Doc. A/810, p. 71; cf. in this respect The right to privacy in the digital age, UN General Assembly Resolution 68/167 of 18 December 2013, UN Doc. A/Res/68/167 (2014), no. 4). Insofar, it needs to be considered in particular whether limitations resulting from the principle of purpose limitation, the requirement to delete the recorded data as well as fundamental requirements regarding oversight and data security are at least observed in general terms. The relevant standards for this appraisal are the domestic laws and the international obligations of the receiving state as well as their actual day-to-day application (cf. similarly ECJ, Judgment of 6 October 2015 – C-362/14 –, Schrems/Digital Rights Ireland, NJW 2015, p. 3151 <3157>, para. 75). 335

(b) In view of the fear of potential human rights abuses through the use of the data in the receiving state, it must be guaranteed in particular that the data will neither be used for political persecution nor inhuman or degrading punishment or treatment (cf. Art. 16a sec. 3 GG). Overall, the legislature must ensure that the transfer of data collected by German authorities and transferred to third countries or international organisations does not undermine the protection of the European Convention on Human Rights and the other international human rights conventions (cf. Art. 1 sec. 2 GG). 336

(2) Whether the required protection level is guaranteed in the receiving state need not be examined separately for each individual case and secured through individually assured commitments that are binding under international law. In this respect, the legislature may instead also rely on a generalising factual assessment rendered by the Federal Criminal Police Office regarding the legal and factual situation in the receiving states. This assessment may claim validity as long as it is not opposed by facts to the contrary in special circumstances (cf. BVerfG, Order of the Second Senate of 15 December 2015 – 2 BvR 2735/14 – para. 69, with further references). 337

If decisions with a view to a receiving state cannot be based on such assessments, it is necessary to conduct a facts-based case-by-case assessment that determines whether it is at least guaranteed that essential requirements for the handling of data are sufficiently met (see above, D IV 1 b bb (1)). If necessary, binding individual guarantees can and must be provided. As a rule, a binding assurance is a suitable means for removing concerns with regard to the permissibility of the transfer of data, so long as it is not to be expected that the assurance will not be adhered to in the individual case (cf. BVerfGE 63, 215 <224>; 109, 38 <62>; BVerfG, Order of the Second Senate of 15 December 2015 – 2 BvR 2735/14 – para. 70). However, as far as the individually applicable requirements are concerned, the legislature may also choose to determine these on the basis of an appraisal of the individual case. 338

Ascertaining that the required degree of protection is met – be it generalised, be it in the individual case – is not a decision at the German authorities' free political disposal. In fact, the decision must be based on substantial and realistic information and must be updated regularly. Its reasons must be documented in a comprehensible manner. Further requirements are that the Federal Data Protection Commissioner has the opportunity to review the decision and that it may be subjected to judicial review (cf. also ECJ, Judgment of 6 October 2015 – C-362/14 –, Schrems/Digital Rights Ireland, NJW 2015, p. 3151 <3156>, paras. 78, 81, 89). 339

cc) Even so, requirements of effective supervisory control including the suitable documentation of the respective transfer activities as well as the requirement of reporting duties apply in Germany (see above, C IV 6 d, e). 340

dd) The standards developed above must be statutorily enshrined in a manner that satisfies the principle of specificity and legal clarity. This also includes the fact that the legal bases which, insofar as permissible, are meant to authorise a transfer of data for the purpose of receiving information through a matching of data collected by authorities in third countries as well as a return of supplementary information are as such designed with legal clarity. 341

2. The transfer requirements stipulated in § 14 sec. 1 sentence 1 nos. 1 and 3 and sentence 2 BKAG are incompatible with these requirements. 342

a) Insofar as it is to be understood as constituting an own legal basis […], § 14 sec. 1 sentence 1 no. 1 BKAG does not satisfy the constitutional requirements for a change in purpose. By generally allowing a transfer of data by the Federal Criminal Police Office for the purpose of fulfilling the tasks incumbent upon it, it lacks standards ensuring that data stemming from particularly intrusive surveillance measures may only be transferred for purposes that conform to the criterion of a hypothetical re-collection of data (cf. above, D I 2 b). Thus the power is not sufficiently delimited and disproportionate. 343

b) With respect to data stemming from the surveillance of private homes, § 14 sec. 1 sentence 1 no. 3 BKAG, too, is too broad and thus incompatible with constitutional requirements. According to the standards developed above, it must be ensured that such data may only be transferred in the event of imminent danger (see above, D I 2 b bb; cf. also BVerfGE 109, 279 <377, 379>). The provision does not contain such a limitation. 344

Yet as far as other data is concerned, the provision is not constitutionally objectionable when construed appropriately. […] 345

c) Finally, the transfer requirements set down in § 14 sec. 1 sentence 2 BKAG are also not compatible with the requirements for a change in purpose. 346

The provision fails to sufficiently ensure that the transfer of data, following the criterion of a hypothetical re-collection of data, is limited to the protection of sufficiently weighty legal interests (cf. above, D I 2 b). The provision generally allows a transfer of data to prevent criminal offences of particular seriousness, without distinguishing with respect to the respective means chosen for the collection of the data. This threshold, however, does not justify the transfer of data stemming from particularly intrusive measures. If the legislature, in the context of data transfers for the purpose of preventing threats – as it does here for the prevention of criminal offences – does not invoke legal interests to determine the new purposes but rather refers to the nature of the crimes it intends to prevent, the respective weightings that apply to data collection under criminal procedural law are relevant here, too. Accordingly, the transfer of data stemming from telecommunications surveillance measures is limited to the prevention of serious criminal offences, while the transfer of data stemming from the surveillance of private homes and remote searches is limited to the prevention of particularly serious criminal offences (cf. BVerfGE 109, 279, <343 et seq.>; 125, 260 <328 and 329>; 129, 208 <243>; see also above, C IV 1 a). The provision, however, does not stipulate such requirements with regard to the transfer of data. 347

Furthermore, in terms of the necessary degree of specificity of the risk situation, the provision does not meet the constitutional requirements in all respects. By indiscriminately allowing a transfer of data as soon as there are “grounds for believing” that a criminal offence will be committed in the future, it also allows a transfer of data obtained through the surveillance of private homes and remote searches without requiring an imminent danger (cf. BVerfGE 109, 279 <377, 379> on the surveillance of private homes) or a sufficiently specific impending danger (cf. BVerfGE 120, 274 <326, 328 and 329> on remote searches). This is incompatible with the requirements set out above (cf. above, D I 2 b bb). However, insofar as other types of data are concerned this interference threshold is not objectionable. As the provision requires indications that a crime will be committed, the transfer of data is conditional on whether a specific evidentiary basis for further investigations arises from the data. This is compatible with constitutional requirements. 348

d) In contrast, the overarching rule in § 14 sec. 7 BKAG does not raise effective constitutional concerns. 349

aa) § 14 sec. 7 sentence 7 BKAG determines that the transfer of data is barred insofar as the person concerned has a prevailing and legitimate interest in halting the transfer; thus, the provision leaves sufficient room for the constitutionally required ascertainment as to whether the required human rights standards are adhered to. 350

bb) § 14 sec. 7 BKAG takes account of the Basic Law’s data protection requirements by setting out procedural law standards for the transfer and by requiring an ascertainment of an appropriate level of data protection in the receiving country. 351

(1) The provision establishes the Federal Criminal Police Office’s responsibility for the admissibility of the transfer of data and thus demands an examination in particular as to whether sufficiently plausible indications result from the transferred information itself or in the context of a transfer request according to which the transfer of data is permissible for the respective purposes. If construed appropriately, the provision ensures both that the transfer purpose is formally communicated and that it is clearly pointed out 352

that the data may be used only for this indicated purpose. In this respect, it is not objectionable that the purpose limitation is secured only by means of a reference to it, rather than by means of a formal obligation; nor is it objectionable that with regard to the deletion period only an informational notice on the German legal situation must be provided. Generally it is sufficient that, with regard to the factual and legal situation in the receiving state, the authorities ascertain that the data protection level is in actual fact appropriate.

(2) § 14 sec. 7 sentences 7 to 9 BKAG stipulates such ascertainment requirements. This provision, when 353
interpreted in conformity with the Constitution, is compatible with the constitutional requirements. It prohibits the transfer of data if a balancing of interests in the individual case results in the finding that legitimate interests of the person concerned prevail and, to that end, notes that these include an appropriate level of data protection in the receiving state. When interpreted in the light of the Constitution, however, the adherence in the receiving state to the fundamental rights requirements requiring appropriate data protection when handling data is not merely a factor the authorities can discretionarily overcome on a case-by-case basis. Instead, minimum fundamental rights requirements must always be ensured. If it is not possible by other means to ascertain that the transferred data will be handled in acceptable conformity with fundamental rule-of-law principles in the third country, recourse must be taken in individual cases to obtaining assurances that meet the requirements set out in § 14 sec. 7 sentence 9 BKAG. Such an interpretation of the provision does not raise concerns as to its constitutionality. The general provision § 27 sec. 1 no. 1 BKAG is an additional backup for the provision.

e) As for the rest, the transfer rules set out in § 14 sec. 1 BKAG do not meet the constitutional 354
requirements insofar as, with regard to transfer practices, they lack sufficient rules on supervisory control and the ordering of reporting duties (see above, C VI 6 d, e). In contrast, documentation requirements are set out in § 14 sec. 7 sentence 3 BKAG as constitutionally required (cf. BVerfGE 133, 277 <370 para. 215>). In light of the fact that § 19 Federal Data Protection Act (*Bundesdatenschutzgesetz*) applies, the data subjects' rights to information are also provided for (cf. BVerfGE 120, 351 <364 and 365>; see above, C IV 6 b; C VI 3 b).

E.

I.

1. The finding that certain provisions are unconstitutional generally results in their voidness. However, 355
the Federal Constitutional Court may also – pursuant to § 31 sec. 2 sentences 2 and 3 of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG) – confine itself to simply declaring that an unconstitutional provision is incompatible with the Constitution (BVerfGE 109, 190 <235>). This results in a mere contestation of the unconstitutionality of a provision without the declaration of its voidness. At the same time, the Federal Constitutional Court may combine the declaration that a provision is incompatible with the Constitution with an order according to which the unconstitutional provision shall nonetheless stay in effect on an interim basis until a date specified by the Court. This option is feasible if the immediate voidness of the contested provision would deprive common goods of paramount importance of their protection and if the outcome of a weighing of these interests with the fundamental rights at stake is that the interference can be tolerated during a transitional period (BVerfGE 33, 1 <13>; 33, 303 <347 and 348>; 40, 276 <283>; 41, 251 <266 et seq.>; 51, 268 <290 et seq.>; 109, 190 <235 and 236>). During the transitional period, the Federal Constitutional Court may, until the constitutional order is restored, take interim measures to reduce the authorities' powers, in line with what appears necessary in light of the weighing of interests (BVerfGE 40, 276 <283>; 41, 251 <267>).

2. Accordingly, § 20h sec. 1 no. 1 c and § 20v sec. 6 sentence 5 BKAG are to be declared 356
unconstitutional and void. The provisions do not satisfy the constitutional requirements and the legislature cannot remedy this by adopting a provision with comparable legislative content.

In contrast, § 20g secs. 1 to 3, §§ 20h, 20j, 20k, 20l, § 20m secs. 1 and 3 – in this respect also § 20v sec. 6 sentence 3 (second half) – and § 20u secs. 1 and 2 as well as § 20v sec. 4 sentence 2, sec. 5 sentences 1 to 4 (without sentence 3 no. 2), § 14 sec. 1 sentence 1 nos. 1 and 3, sentence 2 BKAG are merely declared to be incompatible with the Constitution; the declaration that the provisions are incompatible with the Constitution is combined with the order that they shall nonetheless stay in effect on an interim basis until 30 June 2018 at the latest. The grounds for the unconstitutionality of the provisions do not affect the core of the powers granted through the provisions but merely touch upon individual aspects of their design in light of the rule of law; the fact that the overall assessment resulted in the finding of unconstitutionality is largely due to the fact that there is a lack of individual provisions capable of ensuring proportionality in a comprehensive manner, such as provisions guaranteeing effective review. Under such circumstances, the legislature is given the opportunity to remedy the constitutional contestations and thereby achieve the core of the objectives pursued by the provisions. In light of the great importance of an effective fight against international terrorism for a free and democratic state based on the rule of law, the provisions' continued interim applicability is more tolerable than a declaration of their voidness; a declaration to that effect would deprive the Federal Criminal Police Office of pivotal investigative powers for fighting international terrorism until the adoption of new legislation. 357

However, with regard to the fundamental rights at issue, the order that the provisions are subject to continued applicability, for an interim period, necessitates certain restrictive requirements. A necessary order is, first of all, that measures adopted pursuant to § 20g sec. 2 nos. 1, 2 b, 4 and 5 BKAG may only by ordered by a court; in case of immediate danger, § 20g sec. 3 sentences 2 to 4 BKAG applies accordingly. Furthermore, measures set out in § 20g sec. 1 no. 2, § 20l sec. 1 no. 2 and § 20m sec. 1 no. 2 BKAG may only be ordered if the conditions stipulated in § 20k sec. 1 sentence 2 BKAG are fulfilled in the sense of the interpretation in conformity with the Constitution laid out in the grounds of this decision. Finally, the further use of data pursuant to § 20v sec. 4 sentence 2 BKAG or the transfer of data pursuant to § 20v sec. 5 and § 14 sec. 1 BKAG is, with regard to data stemming from the surveillance of private homes (§ 20h BKAG), only permissible in cases of imminent danger and, with regard to data stemming from remote searches (§ 20k BKAG), only permissible if there is, a sufficiently specific impending danger to the relevant legal interests in that particular case. 358

II.

In parts, the decision was not adopted unanimously. This is true in particular with regard to the finding that § 20g sec. 1 no. 2, § 20l sec. 1 no. 2 and § 20m sec. 1 no. 2 BKAG are unconstitutional (rather than ruling that they may be interpreted in conformity with the Constitution); the recognition that the investigative powers set out in § 20g BKAG typically affect the core area; the objections raised against insufficiently designed supervisory powers, reporting and sanctioning duties; and, in parts, also with regard to the lack of requirements of a judicial decision. These findings were handed down with 5:3 votes. 359

The decision on the reimbursement of expenses is based on § 34a sec. 2 BVerfGG. 360

Kirchhof Gaier Eichberger
Schluckebier Masing Paulus
Baer Britz

[*Excerpt from press release no. 19/2016 of 20 April 2016*]

Separate Opinion of Justice Eichberger:

I cannot subscribe to the decision, in several respects concerning the conclusions drawn with regard to the challenged norms, and in parts of the reasoning.

The decision indeed moves within the framework of the case-law developed by the Court particularly over the past twelve years on the permissibility of interferences with fundamental freedoms for reasons of security, which is to be guaranteed by the state. However, the principles set out by the Senate today, as in the past, almost exclusively derive from the considerations carried out in the context of the proportionality test with a view to balancing the burdens imposed by serious measures upon the fundamental rights of the parties affected, on the one hand, and the state's duties of protection with regard to terrorist threats, on the other. Yet here, too, the prerogative of appraisal with regard to the actual assessment of the risk situation and the prognosis of its development belongs to the legislature. In light of this, the Senate should not have set up such detailed requirements. In weighing the latent threat posed by covert surveillance and investigative measures, it must be kept in mind that most of the challenged norms do not authorise a general collection of data affecting a wide range of persons. Should, in a specific case of the carrying out of investigative measures, persons be affected to whom one can attribute little or no responsibility for the grounds of the investigation, a particular sacrifice is exacted of them as a citizen's duty for the public guarantee of security.

Not all of the procedural, transparency and oversight requirements prescribed to the legislature – even if many of them make sense and may be right – are actually required exactly so by the Constitution. The judgment, despite its welcome steps toward consolidation, nevertheless leads to a problematic entrenchment of the excessive constitutional requirements in this field.

I consider it to be too far-reaching to derive from the principle of proportionality the requirements that persons affected by serious surveillance measures must be given effective sanctioning mechanisms; that the oversight of data collection and use must be carried out in regular intervals no longer than two years; and that reporting duties vis-à-vis Parliament and the public to ensure transparency and oversight must be provided. It would have been sufficient to merely prescribe the level of protection to be ensured by the legislature.

Insofar as the Senate considers the authorisation to carry out certain investigative and data collection measures for the purposes of the prevention of crime to be too unspecific and disproportionate, it needlessly fails to choose the possible option of an interpretation in conformity with the Constitution. Unlike the Senate, I consider the concept chosen by the legislature, to only require a judicial decision for an extension of the majority of the surveillance measures in § 20g sec. 2 BKAG, to be constitutionally tenable. Furthermore, I cannot share the Senate's view that § 20g BKAG is also unconstitutional for not containing any provision for the protection of the core area of private life.

With regard to the use of data obtained by means of surveillance measures, the judgment refines and consolidates the idea of a "hypothetical re-collection" as the notional base for determining the conditions for a change in purpose. I cannot back the exception called for by this concept, whereby every further use and change in purpose with regard to data from the surveillance of private homes or remote searches must be justified by an imminent or a sufficiently specific danger, just as for the initial collection of the data. Even in the context of the surveillance of private homes, the actual massive interference with privacy takes place when the investigation accesses the protected area. A further use – even one with a change in purpose – does indeed perpetuate this interference, but, even with regard to the surveillance of private homes (and similarly with remote searches), it does not reach the level of severity of the initial interference. The further use and change in purpose of intelligence obtained from surveillance measures must thus be subject to the general rules. The Senate should have corrected its existing case-law accordingly.

Separate Opinion of Justice Schluckebier:

Insofar as the decision objects to the challenged provisions for constitutional reasons, I cannot agree to large parts of the decision and the accompanying reasoning. In my opinion, the proportionality test applied in the decision is constitutionally misguided in several respects. Furthermore, the requirements

established for the specificity of individual provisions are excessive. Ultimately, by means of numerous detailed requirements of a technical legislative nature the Senate puts its own notion of regulatory framework before those of the democratically legitimised legislature; however, as far as I am concerned, the Senate goes too far in doing so. Contrary to what the Senate assumed, some of the challenged provisions could in fact have been interpreted in conformity with the Constitution.

Generally it should be borne in mind that the legislature's regulatory approach has essentially found an appropriate and tenable balance in the complex tension between the fundamental rights of persons affected by the police measures on the one hand, and the legislature's obligation to protect the fundamental rights of individuals and the constitutionally protected legal interests of the general public on the other hand. The legislature thus takes into account that, in a state governed by the rule of law, individuals must be able to rely on receiving effective protection by the state and on the protection of guaranteed fundamental freedoms against the state.

The Senate objects to the lack of an explicit statutory provision protecting the core area of private life particularly with regard to special methods for the collection of data outside of private homes (§ 20g Abs. 2 BKAG); in my opinion, such an express provision is not necessary. Indeed, the affected persons are "in public" when they are not inside private homes. However, in those cases, they are not situated in specially protected private areas. The protection of the core area can be ensured at the level of the actual application of the law.

Furthermore, I do not share the reasoning with regard to the requested establishment of an "independent body" that is essentially staffed with external persons who are not entrusted with security functions and is, in respect of collection and evaluation, responsible for actually carrying out and adopting decisions on measures for the surveillance of private homes and remote searches. Given its complicated nature, the Senate's suggested solution affects the effectiveness of the measures since the evaluation of findings is often very urgent and needed as quickly as possible in the context of the prevention of criminal offences and the protection against threats. For that reason, it does not sufficiently satisfy the requirements of appropriateness with regard to the effective prevention of terrorist crimes. The possibility offered to the legislature, to grant the Federal Criminal Police Office "certain short-term initial possibilities of taking action" in exceptional cases where danger will occur unless action is taken,– a case which, in practice, will occur rather often –, clearly contrasts the judgments' assumption according to which the data's special need for protection requires, as a rule, the almost complete exclusion of the Federal Criminal Police Office from the responsibility of initial review.

Insofar as the Senate assumes that the powers to a further use of the data collected in the context of the protection against threats from terrorism and the transfer of such data to domestic authorities and authorities in third countries are unconstitutional in several respects, I cannot fully agree to this either. This applies in particular insofar as the Senate states that it will permit the use of lawfully collected data in further contexts only in order to protect the same or equally important legally protected interests. The judgment predicates the transfer and use of the data for other purposes on whether, even after a change in purpose, this data serves to protect legally protected interests or to uncover criminal offences of such a weight that this could, by constitutional standards, justify collecting them again with comparably weighty means (criterion of a hypothetical re-collection of data). This perspective may be justified with regard to findings that were obtained through highly intrusive, particularly significant interferences, which is the case, for example, when measures such as the surveillance of private homes and remote searches were employed. However, with regard to other interferences, which result in so-called coincidental findings, this can, in my opinion, lead to hardly tolerable results since it requires the rule-of-law order to accept the occurrence of crimes and damage to legally protected interests. On condition that such coincidental findings were obtained through a lawful and thus also constitutional interference, my view is that it is an unacceptable consequence that a state under the rule of law is forced to deliberately "look away". This deprives the potentially concerned individuals or the legally protected interests of the necessary protection

while giving priority to the protection of the data of those persons whom the measures at issue actually target, especially given that this case does not concern a scenario of a change in purpose of mass data that was collected without cause and very broadly.

As for the additional statutory provisions called for by the Senate with regard to the transfer of data to authorities in other countries, I do not share the view that these are constitutionally required. The relevant provision (§ 14 BKAG) could have been interpreted in conformity with the Constitution. The provision explicitly states that the transfer of personal data is prohibited if there are reasons to believe that the data could be used in a manner which would violate the purpose of a German law or if, in the individual case, the protection-worthy interests of the person concerned prevail. This includes the existence of an appropriate data protection standard in the receiving state. The Act also contains transfer prohibitions and grounds for denial (§ 27 BKAG). With these, it can easily be ensured that the transfer of data does not in any way promote human rights violations in other states and that a prior ascertainment of the use of the transferred data in the receiving country takes place. Also in this context, the specifications in the regulatory framework which the legislature is now forced to create will inflate the text of this Act which is already inundated, badly legible and hardly comprehensible, leading to the opposite of norm specificity. However, in its practical application, there will not be any corresponding notable increase in the protection of the persons concerned.

[*End of excerpt*]