Headnotes

to the judgment of the First Senate of 24 April 2013

1 BvR 1215/07

1. **The counter-terrorism database, in the form of a joint database of various security agencies with the purpose of combating international terrorism, which is essentially limited to facilitating access to information, and stipulates that the data may be used for operational tasks only in urgent and exceptional cases, is in its fundamental design compatible with the Constitution.**

2. **Under the fundamental right to informational self-determination, provisions that permit the transfer of information between the police and intelligence services are subject to heightened constitutional requirements. From the fundamental rights follows a principle of separation of information (*informationelles Trennungsprinzip*) that permits such transfers only in exceptional cases.**

3. **With regard to the data to be included and their potential uses, a joint database shared among security agencies, such as the counter-terrorism database, must have a legal design that is sufficiently specific and conforms to the prohibition of disproportionate measures. The Counter-Terrorism Database Act does not fully meet this requirement, namely with regard to the following issues: the identification of the participating agencies, the range of persons included as affiliated with terrorism, the inclusion of contact persons, the use of covertly provided extended basic data, the authorisation of security agencies to define the specific rules for using the data to be stored, and the guarantee of effective supervision.**

4. **The unrestricted inclusion in the counter-terrorism database of data that were collected by interfering with the privacy of correspondence and telecommunications and the right to the inviolability of the home violates Art. 10 sec. 1 and Art. 13 sec. 1 GG.**

FEDERAL CONSTITUTIONAL COURT

– 1 BvR 1215/07 –

Delivered
on 24 April 2013
Ms Sommer
Regierungshauptsekretärin
as Registrar
of the Court Registry

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaint

of Mr S…,

– authorised representative: Rechtsanwalt […] –

against the Act on Setting up a Standardised Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the *Laender* (*Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern* – ATDG, Counter-Terrorism Database Act) of 22 December 2006 (Federal Law Gazette, *Bundesgesetzblatt* – BGBl I p. 3409)

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 6 November 2012 as follows:

Judgment

1. **a) § 1 section 2 and § 2 sentence 1 number 3 of the Act on Setting up a Standardised Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the *Laender* (the Counter-Terrorism Database Act) of 22 December 2006 (Federal Law Gazette I page 3409) are incompatible with Article 2 section 1 in conjunction with Article 1 section 1 of the Basic Law.**

   b) § 2 sentence 1 number 1 letter b, with reference to the support for a supporting group, and § 2 sentence 1 no. 2 of the Counter-Terrorism Database Act, with regard to the criterion "advocacy", are incompatible with Article 2 section 1 in conjunction with Article 1 section 1 of the Basic Law.

   c) § 5 section 1 sentence 2 number 1a of the Counter-Terrorism Database Act is incompatible with Article 2 section 1 in conjunction with Article 1 section 1 of the Basic Law to the extent that information under § 3 section 1 number 1a of the Counter-Terrorism Database Act can be accessed when a search of the extended basic data yields a match.

   d) § 3 section 1 sentence 1 number 1b and § 10 section 1 of the Counter-Terrorism Database Act are incompatible with Article 2 section 1 in conjunction with Article 1 section 1 of the Basic Law, to the extent that they lack the supplementary provisions as laid out in the Reasons.

   e) § 2 sentence 1 number 2 and § 10 section 1 of the Counter-Terrorism Database Act are otherwise to be interpreted in conformity with the Constitution as laid out in the Reasons.

2. **§ 2 sentence 1 numbers 1 to 3, § 3 section 1 number 1, § 5 sections 1 and 2 and § 6 sections 1 and 2 of the Counter-Terrorism Database Act are incompatible with Article 10 section 1 and Article 13 section 1 of the Basic Law insofar as they extend to covertly stored data not covered by § 4 of the Counter-Terrorism Database Act that derive from interferences with the secrecy of telecommunications and the fundamental right to the inviolability of the home.**

3. **Until new provisions are enacted, but no later than 31 December 2014, the provisions held to be incompatible with the Basic Law shall remain in force, subject to the following conditions: Except in an emergency as defined in § 5 section 2 of the Counter-Terrorism Database Act, the use of the counter-terrorism database shall only be permissible if there can be no access to the data of contact persons (§ 2 sentence 1 number 3 of the Counter-Terrorism Database Act) and to data deriving from interferences with the secrecy of telecommunications and the fundamental right to inviolability of the home, and if it is guaranteed that for searches relating to extended basic data, only information as provided in § 3 section 1 number 3 of the Counter-Terrorism Database Act can be accessed; as soon as the access to the data of contact persons, and to data that derive from interferences with the secrecy of telecommunications and the fundamental right to the inviolability of the home is blocked, these data may no longer be used, not even in an emergency under § 5 section 2 of the Counter-Terrorism Database Act.**

4. **The remainder of the constitutional complaint is rejected as unfounded.**

5. **[…]**

Reasons:

A.

The constitutional complaint concerns the constitutionality of the Counter-Terrorism Database Act. 1

I.

The complainant challenges the Act on Setting up a Standardised Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the *Laender* (Counter-Terrorism Database Act – ATDG) enacted as Art. 1 of the Act on Setting up Joint Databases of Police Authorities and Intelligence Services of the Federal Government and the *Laender* (*Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder*, Joint Databases Act) of 22 December 2006 (BGBl I p. 3409). […] 2

1. The Counter-Terrorism Database Act laid down the legal basis for the counter-terrorism database, a joint database of the police and intelligence services of the Federal Government and the federal states, or *Laender*, serving to combat international terrorism. This database facilitates and accelerates the transfer of information between the participating police and intelligence services by allowing certain information related to the fight against international terrorism, which is held by the individual agencies, to be found more quickly and accessed more easily by all participating agencies. 3

a) § 1 ATDG determines that the counter-terrorism database is to be maintained as a joint, standardised, central database by the Federal Criminal Police Office (*Bundeskriminalamt*) and defines the agencies that may participate in it. […] 4

b) § 2 ATDG determines that, and with regard to which persons or objects, agencies are obliged to store previously collected data in the counter-terrorism database. […] 5

c) Which data are to be stored on the persons and objects mentioned in § 2 sentence 1 nos. 1 to 4 ATDG follows from § 3 sec. 1 ATDG. This provision distinguishes between the basic data listed in § 3 sec. 1 no. 1a ATDG (hereafter, for clarity's sake, also called "simple basic data") and the extended basic data listed in § 3 sec. 1 no. 1b ATDG. 6

[…] 7-9

§ 4 ATDG permits limited or covert storage of data where required by a particular interest in confidentiality or the legitimate interests of the person concerned. […] 10

d) § 5 sec. 1 ATDG governs access to the stored data in standard cases. […] 11

Under § 6 sec. 1 sentence 1 ATDG, the requesting authority may use the data to which it received access under § 5 sec. 1 ATDG only to examine whether the match is associated with the person being sought, and to prepare and substantiate a request for an individual data transfer. 12

e) For emergencies, § 5 sec. 2 sentence 1 ATDG authorises the requesting authority to access the extended basic data directly from a match. […] 13

If the requesting authority has obtained access to data in an emergency, § 6 sec. 2 ATDG permits their use only where this is indispensable in order to avert a current threat in connection with the fight against international terrorism. […] 14

§ 7 ATDG provides that the transfer of findings following a request according to § 6 sec. 1 sentence 1 ATDG is governed by the respective current rules on data transfer. 15

f) § 8 ATDG divides the responsibility for data protection between the authority that entered the data and the requesting authority. […] 16

§ 10 sec. 2 ATDG governs the release of information to the persons concerned. This provision distinguishes between data stored openly and data stored covertly, [translator's note: i.e. such that are directly accessible and such that will only be disclosed subject to a certain procedure]. […] 17

Finally, § 11 ATDG contains requirements for the correction, deletion and blocking of access to data, while § 12 ATDG governs what details are to be specified by the Federal Criminal Police Office in an order to open a data file. […] 18

g) […] 19

2. The provisions of the Counter-Terrorism Database Act of 22 December 2006 20

(BGBl I p. 3409), as amended by Article 5 of the Act of 26 February 2008 (BGBl I p. 215) which are relevant for this case read as follows:

[*The Federal Ministry of the Interior provides a translation of the Counter-Terrorism Database Act in its version of 22 December 2006 at the following web address: http://www.bmi.bund.de/SharedDocs/Gesetzestexte/DE/Antiterrordateigesetz_en.pdf?__blob=publicationFile (last accessed 30 April 2015); the relevant provisions are reproduced with kind permission. § 1 sec. 1 has been amended by Article 5 of the Act of 26 February 2008; the amended passage (in bold type) has been retranslated by the Federal Constitutional Court.*]

Section 1 [*The translation of the Counter-Terrorism Database Act provided by the Federal Ministry of the Interior uses "Section" for "§","paragraph" for "section", "subpara." for "letter" and "data protection" for "data privacy".*] 21

Counter-terrorism database

(1) To discharge their legal duties of investigating and fighting international terrorism affecting the Federal Republic of Germany, the participating authorities, i.e. the Federal Criminal Police Office (BKA), **the federal police authority designated in the regulation enacted pursuant to Section 58(1) of the Federal Police Act,** the *Land* Criminal Police Offices (LKA), the Federal and *Land* Offices for the Protection of the Constitution, the Military Counter-Intelligence Service (MAD), the Federal Intelligence Service (BND) and the Customs Criminological Office (ZKA), shall run a joint standardized central counter-terrorism database (counter-terrorism database).

(2) Other police authorities, in consultation with the Federal Ministry of the Interior, shall be entitled to participate in the counter-terrorism database if

1. they are assigned tasks of fighting international terrorism affecting the Federal Republic of Germany not only in individual cases,

2. they need access to the counter-terrorism database to discharge their duties pursuant to no. 1, and if this is appropriate with regard to the protected interests of the persons concerned and the security interests of the participating authorities.

Section 2 22

Contents of the counter-terrorism database and storage obligation

If data pursuant to Section 3(1) have already been collected, the participating authorities are obliged to store these data in the counter-terrorism database if the authorities have information from the police or intelligence services (intelligence) which clearly indicates that the data refer to

1. persons who participate in or support

a) a terrorist organization pursuant to Section 129(a) of the German Criminal Code acting at an international level, or a terrorist organization pursuant to Section 129(a) in conjunction with Section 129(b)(1)(1) of the German Criminal Code acting in the

Federal Republic of Germany, or

b) a group which supports an organization pursuant to sub-para. (a),

2. persons who unlawfully use violence to enforce political or religious interests or who support, prepare, advocate or intentionally incite such use of violence,

3. persons when there is evidence that they have more than superficial or coincidental contact with persons under no. 1(a) or no. 2, and through whom further information for investigating and fighting international terrorism can be obtained (contact persons),

or

4. (…)

and knowledge of these data is necessary to investigate and fight international terrorism affecting the Federal Republic of Germany. The first sentence applies only to data which the participating authorities may process in an automated way in compliance with the relevant legislation.

Section 3 23

Types of data to be stored

(1) The following types of data, if available, shall be stored in the counter-terrorism database:

1. Personal data

a) pursuant to Section 2(1) nos. 1 to 3: surname, first name, previous names, other names, aliases, divergent spellings of names, sex, date of birth, place of birth, country of birth, current and previous nationalities, current and previous addresses, special physical features, languages, dialects, photographs, name of the category pursuant to Section 2, and information on identity documents (basic data) if this does not violate other legal provisions and is necessary to identify a person.

b) the following types of data (extended basic data) pursuant to Section 2(1) nos. 1 and 2 and on contact persons when there is evidence that they are aware of the planning or commission of an offence under Section 2(1) no. 1(a) or of the use, support or preparation of unlawful violence within the meaning of Section 2(1) no. 2:

aa) telephone numbers and terminal devices in their own possession or used by them,

bb) e-mail addresses,

cc) banking data,

dd) safe deposit boxes,

ee) vehicles registered under the person’s name or used by the person,

ff) marital status,

gg) ethnic origin,

hh) data on religious affiliation if necessary in an individual case to investigate or combat international terrorism,

ii) special skills, which according to intelligence of participating authorities – based on specific facts – may be used for preparing and carrying out terrorist acts pursuant to Section 129(a)(1) and (2) of the German Criminal Code, in particular special knowledge and skills in the production or handling of explosives or weapons,

jj) data on school qualifications, occupational qualifications and occupations pursued,

kk) data on a current or previous activity in a vital institution in the meaning of Section 1 (5) of the Security Clearance Check Act or in a transport company or utility, a means of public transport or official building,

ll) data referring to the threat posed by a given person, in particular if he/she possesses a weapon or is prepared to use violence,

mm) driving or pilot's licence,

nn) places or regions visited where persons listed in Section 2(1) nos. 1 and 2 meet,

oo) contact persons pursuant to Section 2(1) no. 3 for the persons listed in Section 2(1) no. 1(a) or no. 2,

pp) the name of the specific organization or group pursuant to Section 2(1) no. 1 (a) or (b),

qq) the date of the latest event which was the reason for storing the intelligence, and

rr) special summarizing remarks based on evidence, additional considerations and assessments of basic data and extended basic data already stored in databases of the participating authorities if this is necessary after due consideration and essential to investigate or combat international terrorism,

2. (…)

3. in addition to the data under nos. 1 and 2, information about the authority possessing the intelligence, the file reference or other reference codes, and the classification, if available.

(2) If data to be stored have to be labelled in line with other legal provisions, this label shall be maintained when storing the data in the counter-terrorism database.

Section 4 24

Restricted and covert storage

(1) As far as special confidentiality concerns so require or if in exceptional cases the affected person's interests meriting protection could be injured, the participating authority may partially or wholly abstain from storage of the extended basic data listed in Section 3(1) no. 1(b) (restricted storage) or enter data on persons, associations, groupings, foundations, companies, property, banking data, addresses, telephone numbers, telecommunications terminal devices, websites, and e-mail addresses listed in Section 2 in such a way that other requesting authorities involved cannot see that these data were stored and thus will not be able to access the stored data (covert storage). The head of the authority in question or an official of the higher service specially designated by the head shall decide about restricted and covert storage.

(2) If a request concerns data in covert storage, the authority which entered the data is automatically informed of the request and receives all relevant information. It shall immediately contact the requesting authority to check whether intelligence pursuant to Section 7 may be transferred. The authority which entered the data may refrain from contacting the requesting authority only if interests of confidentiality outweigh the circumstances of an individual case. The authority shall document the reasons for its decision pursuant to the second sentence. The request for information and the documentation pursuant to the third sentence shall be deleted or destroyed no later than such time as the covertly stored data are deleted.

Section 5

Data access

(1) The participating authorities may use data stored in the counter-terrorism database in an automated procedure as needed to discharge their duties in relation to investigating or combating international terrorism. If a match is found, the requesting authority shall have access to the following:

1. a) when requesting information about a person: the person's basic

personal data stored in the database, or

b) when requesting information about associations, groupings, foundations, companies, property, banking data, addresses, telephone numbers, telecommunications terminal devices, websites or e-mail addresses: stored data pursuant to Section 2(1) no. 4, and

2. data pursuant to Section 3(1) no. 3.

The requesting authority may access extended basic data on persons if the authority which entered the data authorizes such access upon request in individual cases. In such cases, decisions about this case shall be based on the applicable rules governing data transfer.

(2) If a match is found, the requesting authority may directly access extended basic data if necessary due to specific evidence indicating a current threat to the life, limb, health or freedom of a person or property of substantial value, the preservation of

which is in the public interest and if the requested data cannot be transferred in due time (emergency). The head of the authority or an official of the higher service specially designated by him/her shall decide whether the case is an emergency. The decision and the reasons for it shall be documented. The access shall be documented with reference to the decision pursuant to the third sentence. The authority which entered the data shall be immediately asked for subsequent authorization. If subsequent authorization is refused, it is no longer permissible to use these data. The requesting authority shall immediately delete these data or block them pursuant to Section 11(3). If these data were submitted to a third party, the third party shall be immediately informed that it is no longer permissible to use the data.

(3) Within the participating authorities only authorized persons may access the counter-terrorism database.

(4) Each time the database is accessed, the purpose and urgency of the request shall be indicated, documented and recognizable.

Section 6 26

Further use of the data

(1) The requesting authority may use the accessed data solely for the purpose of checking whether the hit matches the person or information sought pursuant to Section 2(1) no. 4 and to request intelligence in order to discharge its duties in relation to investigating or combating international terrorism. Data may be used for purposes other than investigating or combating international terrorism only if

1. this is necessary to prosecute a serious crime or to prevent a threat to the life, limb, health or freedom of a person, and

2. the authority which entered the data authorizes such use.

(2) In case of an emergency, the requesting authority may use the data it has accessed only if this is vital to prevent a current threat pursuant to Section 5(2)(1) in connection with combating international terrorism.

(3) If data are used pursuant to paragraph 1(2) or paragraph 2, they shall be labelled accordingly. After transferring the data the recipient shall maintain the labelling. The same shall apply to labelling pursuant to Section 3(2).

(4) If the Federal Criminal Police Office and the *Land* Criminal Police Offices use the counter-terrorism database at the request or on behalf of the Federal Public Prosecutor, they shall transfer the data to which they have been given access to the Federal Public Prosecutor. The Federal Public Prosecutor may use the data upon request pursuant to paragraph 1(1). Section 487(3) shall apply mutatis mutandis.

Section 7 27

Transfer of intelligence

The transfer of intelligence upon a request pursuant to Section 6(1)(1) between participating authorities shall be governed by the applicable rules on data transfer.

Section 8 28

Responsibility for data protection

(1) The authority which entered the data shall be responsible for protecting the data stored in the counter-terrorism database, namely for seeing that data are collected and entered lawfully, and that the data entered are correct and up to date. The authority which entered the data must be recognizable. The requesting authority shall be responsible for the permissibility of the request.

(2) Only the authority which entered the data may change, correct, block or delete them.

(3) If an authority has reason to believe that data entered by another authority are not correct, it shall immediately inform the authority which entered the data. The latter shall immediately examine this information and correct the data, if necessary.

Section 9 29

Log data, technical and organizational measures

(1) For the purpose of monitoring data protection, the Federal Criminal Police Office shall log the time, the information identifying the requested records, the authority which accessed the database and the purpose of this access pursuant to Section 5(4). The log data may be used only if knowledge thereof is necessary to monitor data protection, to back up data, to ensure proper operation of the data processing system, and to confirm that confidential documents were read. Log data stored solely for the purposes mentioned in the first sentence shall be deleted after 18 months.

(2) The Federal Criminal Police Office shall take the technical and organizational measures required under Section 9 of the Federal Data Protection Act.

Section 10 30

Data protection monitoring, provision of information to the data subject

(1) Pursuant to Section 24(1) of the Federal Data Protection Act, the Federal Commissioner for Data Protection and Freedom of Information shall be responsible for monitoring data protection. The protection of data entered and requested by a *Land* authority shall be governed by the data protection act of the respective *Land*.

(2) Pursuant to Section 19 of the Federal Data Protection Act, the Federal Criminal Police Office, in consultation with the authority responsible for data protection pursuant to Section 8(1)(1) and which examines whether disclosing such information is in line with its legal provisions, shall provide information about data not in covert storage. Disclosure of information on data in covert storage depends on the legal provisions applying to the authority which entered the data.

Section 11 31

Correction, deletion and blocking of data

(1) Incorrect data shall be corrected.

(2) Personal data shall be deleted if their storage is not permissible or if they are not necessary to investigate or combat international terrorism. They shall be deleted no later than such time as the relevant intelligence has to be deleted pursuant to the legal provisions applying to the authorities involved.

(3) Data shall be blocked and not deleted if deletion is likely to harm the interests of the person concerned which are worthy of protection. Blocked data may be requested and used solely for the purpose which justified saving them from deletion. They may also be requested and used if this is necessary to protect significant legal interests, if it would otherwise be impossible or very difficult to clarify the facts of the case, or if the person concerned agrees.

(4) In line with the time limits applying to intelligence data and when processing individual cases, the authorities which enter the data shall examine whether personal data need to be corrected or deleted.

Section 12 32

Order opening a data file

For the joint database, Federal Criminal Police Office in consultation with the participating authorities shall adopt an order opening a data file specifying the following details:

1. areas of international terrorism affecting the Federal Republic of Germany,

2. other police authorities participating pursuant to Section 1(2),

3. type of data subject to storage pursuant to Section 3(1),

4. entry of data to be stored,

5. organizational units of the participating authorities with access rights,

6. categorization of purposes and the urgency of a request,

7. log data.

The order opening a data file shall be approved by the Federal Ministry of the Interior, the Federal Chancellery, the Federal Ministry of Defence, the Federal Ministry of Finance and the supreme *Land* authorities responsible for the participating *Land* authorities. The Federal Commissioner for Data Protection and Freedom of Information shall be consulted before the order opening a data file is adopted.

Section 13 33

Restriction of fundamental rights

The fundamental rights to privacy of correspondence, posts and telecommunications (Article 10 of the Basic Law) and to the inviolability of the home (Article 13 of the Basic Law) shall be restricted under the terms of this Act.

[*End of translation provided by the Federal Ministry of the Interior*]

3. […] 34-37

4. […] 38-39

5. Various data privacy commissioners have performed audits at participating agencies with respect to the counter-terrorism database. The Federal Commissioner for Data Privacy and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) audited data processing at the Federal Criminal Police Office, the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), and the Federal Intelligence Service (*Bundesnachrichtendienst*). He expressed fundamental objections concerning the storage of extended basic data about contact persons, and criticised that the Federal Criminal Police Office transferred data from a source database to the free text field under § 3 sec. 1 no. 1b rr ATDG, without review of each individual case. Thereupon the Federal Criminal Police Office changed its procedure for filling in the free text field (Bundestag Document, *Bundestagsdrucksache* – BTDrucks 16/12600, pp. 51 and 52). At the Federal Office for the Protection of the Constitution, shortcomings were found in the labelling of data deriving from covert telecommunications monitoring, as well as problems with filling in the counter-terrorism database, particularly in the free text field. No formal objection was raised, since the Office consented to correct the discovered shortcomings immediately (BTDrucks 17/5200, pp. 83 and 84). Agencies of the federal states were also audited in reference to the counter-terrorism database, for example in Baden-Württemberg, in the form of on-site audits lasting several days at the Baden-Württemberg *Land* Criminal Police Office (*Landeskriminalamt*) (at the Department for Protection of the State) and the *Land* Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz*). Objections by the *Land* commissioner to shortcomings in reference to some data records resulted in the deletion or correction of those records (*Landtag* of Baden-Württemberg, Landtag Document, *Landtagsdrucksache* – LTDrucks 14/2050, pp. 12 and 14 et seq.). Further audits were performed by the *Land* Commissioners for Data Privacy (*Landesbeauftragte für den Datenschutz*). 40

II.

The complainant claims that the challenged provisions violate his fundamental right to informational self-determination under Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 of the Basic Law (*Grundgesetz* – GG) and his fundamental rights under Art. 10, Art. 13 and Art. 19 sec. 4 GG. 41

[…] 42-51

III.

The Federal Government, the Federal Commissioner for Data Privacy and Freedom of Information, the Schleswig-Holstein Independent *Land* Centre for Data Privacy (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*), the Berlin Commissioner for Data Privacy and Freedom of Information, and the Baden-Württemberg Commissioner for Data Privacy submitted statements on the constitutional complaint. 52

1. The Federal Government holds the view that the constitutional complaint is inadmissible, or at least unfounded. 53

a) […] 54

b) […] 55

aa) […] 56

bb) […] 57

cc) […] 58-63

dd) […] 64-65

ee) […] 66

ff) […] 67

gg) With reference to the facts, the Federal Government states the following: storage primarily concerns persons living in other countries, the spelling of whose names is not always unambiguous. In August 2012, 17,101 data records on persons were stored in the counter-terrorism database, some 920 of which were duplicate mentions or duplicate records, so that approximately 16,180 different persons were affected by the stored records. Of these persons, 2,888 had their residence in Germany and 14,213 persons resided abroad. The large number of persons residing abroad is explained by the participation of the Federal Intelligence Service. Data on 2,833 persons had been stored covertly within the meaning of § 4 sec. 1 sentence 1 ATDG. The participating authorities exercise great restraint in entering contact persons without known terrorist activities in the counter-terrorism database. In August 2012 the database contained only 141 data records for contact persons without indications of malicious intent, entered primarily by *Land* police officials. 68

The existing data records, the Federal Government states, contain hardly any entries in the extended basic data. Only 44% of the data records include any extended basic data at all. Hardly any data record includes an extended basic data record that is even approximately complete. Over 94% of the entries contain nothing in the free text field, in part because the source database of the Federal Intelligence Service does not include a comparable field. The free text field is limited to a total of 2,000 69

characters, or in other words, less than one DIN A 4 page of text. As a rule, the entries are very brief, usually between 15 and 55 characters, and often contain only one word. Only one-third of the personal data records contain more than 100 characters in the free text field under § 3 sec. 1 no. 1b rr ATDG.

From March 2007 to the autumn of 2012, a relatively constant 1,200 search requests per week, or a total of some 350,000 search requests, were recorded. This shows, the Federal Government says, that the counter-terrorism database is being used more as a “specialised telephone book”, and not for a general matching of sources. During this period a request for extended basic data was placed in less than 1% of cases. As a rule, the Federal Government says, it makes more sense for the agencies to directly contact the agency maintaining the record than to ask for extended basic data, which are only in special situations helpful as a first and rapid assessment of dangerousness. Access to extended basic data was refused in an estimated one out of every three or four requests. 70

To permit a reasonable limit on the results, the Federal Government says, the system currently ensures that release is refused through technical means for any request with more than 200 matches. The number of matches resulting from a search averages four to five. Under the emergency provision of § 5 sec. 2 ATDG, only one access to extended basic data took place until August 2012. This was an access by a *Land* Criminal Police Office to a data record of the Federal Office for the Protection of the Constitution. 71

According to the Federal Government, a total of some 7.7 million data records are stored on the log data server; each data record reflects the database transactions triggered by one activity in the counter-terrorism database. 72

2. The Federal Commissioner for Data Privacy and Freedom of Information has concerns about the Counter-Terrorism Database Act. […] 73-74

3. The Schleswig-Holstein Independent *Land* Centre for Data Privacy and the Berlin Commissioner for Data Privacy and Freedom of Information submitted a joint statement. They hold that the constitutional complaint is admissible and well-founded. […] 75-76

4. The Baden-Württemberg *Land* Commissioner for Data Privacy reports on on-site audits at the *Land* Criminal Police Office and the *Land* Office for the Protection of the Constitution in 2007 (cf. *Landtag* of Baden-Württemberg, LTDrucks 14/2050, pp. 12 et seq.) and 2012. […] 77

IV.

[…] 78

B.

The constitutional complaint is admissible. 79

I.

The complainant claims a violation of his fundamental right to informational self-determination under Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG, the secrecy of correspondence and telecommunications under Art. 10 sec. 1 GG, the inviolability of the home under Art. 13 sec. 1 GG and, in conjunction with the above fundamental rights, a violation of the guarantee of the protection of rights under Art. 19 sec. 4 GG. 80

[…] 81

II.

The complainant is concerned directly, individually, and presently by the challenged provisions. 82

1. The complainant does not lack the necessary direct concern. It is true that a complainant is only directly affected by a legal provision if it interferes with the complainant's rights without need for further implementation. If the implementation of a law requires – as a legal requirement or in practice – an implementing measure that is governed by the implementing agency, the complainant must generally first challenge that measure and exhaust all legal remedies before he or she may raise a constitutional complaint (Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 1, 97 <101 et seq.>; 109, 279 <306>; established case-law). However, one must presume a direct concern if the complainant cannot seek recourse to the competent courts because he or she has no knowledge of the respective implementing measure. […] 83

This is not altered by the fact that under § 10 sec. 2 ATDG, the complainant has the option to request information on the storage of data, after which he can seek the protection of the courts against that storage. For he can pursue this course only if data about him are indeed stored at a certain time; he cannot seek – as he does – protection against the possibility that such data are stored at any time without him being able to influence this or to become aware of it. […] 84

2. The complainant is concerned individually and presently. 85

If only the implementation of the challenged law impairs the complainant in a concrete way, but the complainant is not usually informed about the implementing actions, the requirements for being concerned individually and presently are met if the complainant shows that there is some probability that his or her fundamental rights will be affected by the measures arising from the challenged law (cf. BVerfGE 122, 63 <81 and 82>; 125, 260 <305>; established case-law). The required degree of probability depends on the complainant's options for showing that he or she is affected. For instance, it is relevant whether the measure is aimed at a narrowly defined group of persons, or whether the measure has a broad reach and may accidentally include third parties. Statements by which complainants would have to incriminate themselves as criminal offenders, or as the potential instigators of a threat to public safety, cannot be demanded as evidence for their being affected presently and individually 86

(cf. BVerfGE 109, 279 <308>; 113, 348 <363>; 120, 378 <396>).

87 The complainant's arguments satisfy these requirements. It is true that the complainant can only incompletely demonstrate that there is a specific probability that he is affected by the storage of data. Essentially, he only mentions being in contact to persons who may be affiliated with terrorism. However, given the broad range of persons who may be affected by storage of data in the counter-terrorism database, his arguments are still sufficient. Under § 2 sentence 1 ATDG, data are collected not only about persons suspected of terrorism and their supporters, but to a large extent also about persons merely deemed to belong to the environs of persons thought to be involved with terrorism, and even persons who have merely had contact with them – including those who know nothing of any connection between their contact person and terrorism.

C.

88 The constitutional complaint provides no reason for a preliminary ruling from the European Court of Justice under Art. 267 TFEU to clarify the reach of fundamental rights under Union law with regard to the transfer of data among various security agencies in the context of a joint database, such as the one governed by the Counter-Terrorism Database Act. This also applies with regard to the fundamental right to the protection of personal data under Art. 8 of the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights – EUCFR). The European fundamental rights under the EUCFR are not applicable in the case at hand. The challenged provisions must be measured against the fundamental rights under the Basic Law, if only because they are not governed by Union law (cf. BVerfGE 118, 79 <95>; 121, 1 <15>; 125, 260 <306 and 307>; 129, 78 <90 and 91>). Accordingly, this is also not a case of implementation of European Union law, which alone could result in the Member States' being bound by the Charter of Fundamental Rights (Art. 51 sec. 1 sentence 1 EUCFR).

89 However, the challenged provisions do concern enabling a transfer of data in order to combat international terrorism, and therefore raise questions which do in part concern areas that are regulated by Union law. Under Art. 16 TFEU for example, the European Union has powers of its own concerning provisions on data privacy. For example, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ L 281 of 23 November 1995, pp. 31 et seq. – the Data Privacy Directive) states significant requirements for data processing that, in general, apply to both private parties and public authorities. Union law also contains various competences and legal bases related to the protection against terrorism. In particular, Art. 2 of Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ L 253 of 29 September 2005, pp. 22 et seq.) provides that subject to national law, the Member States must transmit to Eurojust, Europol and the other Member States all

relevant information concerning the results of criminal investigations by their criminal prosecution authorities about terrorist offences. The Counter-Terrorism Database Act and the streamlining of cooperation among security agencies that it aims for therefore also has connections with Union law, and if further results are obtained via the transfer of information initiated by the Counter-Terrorism Database Act, the Act indirectly also affects the scope of reporting obligations under Union law. There are also points of connection with Union law regarding the obligations to enact restrictive measures against certain persons and entities in order to combat terrorism under Council Regulation (EC) no. 2580/2001 of 27 December 2001 (OJ L 344 of 28 December 2001, pp. 70 et seq.). In other situations as well can and, where applicable, must the results of the cooperation streamlined by the counter-terrorism database become part of the numerous legal relationships governed by Union law that are part of judicial cooperation.

Nevertheless, it is beyond doubt and requires no further clarification – including under the standards of the *acte claire* case-law of the European Court of Justice (ECJ, judgment of 6 October 1982, Case C-283/81, C.I.L.F.I.T., ECR 1982, p. 3415 paras. 16 et seq.) – that the Counter-Terrorism Database Act and the activities carried out by the public security agencies and intelligence services on that basis are no implementation of Union law within the meaning of Art. 51 sec. 1 sentence 1 EUCFR. With regard to the Data Privacy Directive, this already follows from Art. 3 sec. 2 of Directive 95/46/EC, which makes an express exception for data processing concerning public security, state security, and the activities of the state in areas of criminal law. The establishment and organisation of the counter-terrorism database are also not otherwise governed by Union law. In particular, there is no provision of Union law that obliges the Federal Republic of Germany to establish such a database, impedes it from doing so, or prescribes anything about the content of such a database. Rather, the Counter-Terrorism Database Act pursues nationally defined objectives that can only indirectly affect the functioning of legal relationships governed by Union law; this is insufficient for a review according to the fundamental rights under Union law (cf. ECJ, judgment of 18 December 1997, C-309/96, Annibaldi, ECR 1997, p. I-7493 para. 22). Therefore any applicability of fundamental rights under Union law is excluded from the outset. It follows directly from the wording of Art. 51 sec. 2 EUCFR and from Art. 6 sec. 1 of the Treaty on European Union that the Charter does not extend the field of application of Union law beyond the competences of the Union, and that it neither establishes new powers or tasks for the Union, nor modifies the powers and tasks defined in the Treaties (cf. also ECJ, judgment of 15 November 2011, C-256/11, Dereci et al., para. 71; ECJ, judgment of 8 November 2012, C-40/11, Iida, para. 78; ECJ, judgment of 27 November 2012, C-370/12, Pringle, paras. 179 and 180). 90

Accordingly, for the questions that were raised, and which only concern German fundamental rights, the European Court of Justice is not the lawful judge according to Art. 101 sec. 1 GG. The ECJ's decision in the case Åkerberg Fransson (ECJ, judgment of 26 February 2013, C-617/10) does not change this conclusion. As part of a 91

cooperative relationship between the Federal Constitutional Court and the European Court of Justice (cf. BVerfGE 126, 286 <307>), this decision must not be read in a way that would view it as an apparent ultra vires act or as if it endangered the protection and enforcement of the fundamental rights in the Member States (Art. 23 sec. 1 sentence 1 GG) in a way that questioned the identity of the Basic Law's constitutional order (cf. BVerfGE 89, 155 <188>; 123, 267 <353 and 354>; 125, 260 <324>; 126, 286 <302 et seq.>; 129, 78 <100>). The decision must thus not be understood and applied in such a way that absolutely any connection of a provision's subject-matter to the merely abstract scope of Union law, or merely incidental effects on Union law, would be sufficient for binding the Member States by the Union's fundamental rights set forth in the EUCFR. Rather, the European Court of Justice itself expressly states in this decision that the European fundamental rights under the Charter are "applicable in all situations governed by European Union law, but not outside such situations" (ECJ, judgment of 26 February 2013, C-617/10, para. 19).

D.

The constitutional complaint is, in part, well-founded. 92

I.

The challenged provisions interfere with the protection afforded by the right to informational self-determination (Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG), the right to secrecy of correspondence and telecommunications (Art. 10 sec. 1 GG) and the right to inviolability of the home (Art. 13 sec. 1 GG). 93

1. §§ 1 to 6 ATDG govern the storage and use of personal data, and therefore affect the right to informational self-determination. If the data that were stored and used were obtained by interfering with Art. 10 sec. 1 or Art. 13 sec. 1 GG, their subsequent use must also be measured against these fundamental rights (cf. BVerfGE 125, 260 <313>; established case-law). 94

2. The provisions interfere with these fundamental rights. A first interference lies in that data from different sources are linked together by the obligation to store data under §§ 1 to 4 ATDG. This finding is not invalidated by the fact that the data had already been gathered elsewhere, because the data are being combined and processed according to new criteria so as to make them available to agencies other than those who gathered them, and for those other agencies' purposes. Furthermore, the provisions on the use of the data through searches under §§ 5 and 6 ATDG; on access to the simple basic data in the event of a match under § 5 sec. 1 sentences 1 and 2, § 6 sec. 1 sentence 1 ATDG; and on access to the extended basic data in emergencies under § 5 sec. 2, § 6 sec. 2 ATDG also interfere with these fundamental rights. 95

II.

The challenged provisions are formally compatible with the Constitution. In particu- 96

lar, they do not exceed the limits of the federal powers.

1. Insofar as the Counter-Terrorism Database Act governs the exchange of information between the Federal Criminal Police Office, the *Land* Criminal Police Offices, the Federal Office for the Protection of the Constitution, the *Land* authorities for the protection of the Constitution, and other law enforcement agencies, the Federal Government can base its legislative powers on the competences under Art. 73 sec. 1 nos. 10a to 10c GG, which concern the cooperation among the authorities. […] 97

The competence for regulating the cooperation among the various law enforcement agencies is not limited to criminal prosecution. […] 98

The fact that the Counter-Terrorism Database Act governs the cooperation among police and constitutional protection agencies not only in a substantive way, but also across the agencies, does not mean that one cannot rely on Art. 73 sec. 1 no. 10 GG. […] 99

2. Insofar as § 1 sec. 1 ATDG includes the Federal Intelligence Service, the Military Counter-Intelligence Service, the Customs Criminological Office and the Federal Police as additional authorities, the power to do so is founded on Art. 73 sec. 1 no. 1 and no. 5 GG. 100

The competence to include the Federal Intelligence Service derives from the Federal Government's authority to regulate foreign affairs under Art. 73 sec. 1 no. 1 GG. However, the powers thus conferred on the Federal Government need to be seen in the context of the distribution of other legislative competences. They do not entitle the legislature to confer on the Federal Intelligence Service the power to prevent, hinder or prosecute offences *per se*, merely because the cases have a foreign connection (cf. BVerfGE 100, 313 <368 et seq.>). Provisions can only be based on the legislative powers under Art. 73 sec. 1 no. 1 GG if they are part of a legal and practical context that concerns intelligence activities abroad, and that provides political intelligence to the Federal Government (cf. BVerfGE 100, 313 <370 and 371>). The participation of the Federal Intelligence Service in the counter-terrorism database is compatible with these requirements. […] 101

The Federal Government can base the participation of the Military Counter-Intelligence Service on Art. 73 sec. 1 no. 1 GG (defence) and that of the Federal Police and the Customs Criminological Office on Art. 73 sec. 1 no. 5 GG (protection of customs and borders). […] 102

By contrast, no provision that would directly allow the other agencies participating in the counter-terrorism database to download the data entered by these federal agencies could be based on Art. 73 sec. 1 nos. 1 and 5 GG. Nor does the Counter-Terrorism Database Act include such a provision. Rather, if properly understood, § 5 sec. 1 and 2 ATDG requires separate data collection rules, at the *Land* level if applicable, for the use of the database by each of the agencies accessing it (cf. BVerfGE 125, 260 <315>; 130, 151 <193>). 103

3. […] 104

III.

The counter-terrorism database, which was established by the challenged provisions, is in its fundamental design compatible with the right to informational self-determination under Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG. The principle of proportionality does not fundamentally oppose such a database, which, in the context of investigating and combating international terrorism, serves to initiate the receipt of information, and in emergencies also serves to defend against dangers. However, also its individual provisions detailing the structure of the database must comply with the principle of proportionality. 105

1. The counter-terrorism database has a legitimate aim. It is primarily meant to inform security agencies quickly and easily of whether other security agencies have relevant information about certain persons associated with international terrorism. It thus aims to provide preliminary information with which these agencies can initiate searches of information from other authorities faster and more expediently, and that in emergencies can also permit a first assessment of a threat so as to guide further action. The legislature does not seek a general exchange of personal data among all security agencies, or the elimination of all bounds on information between these agencies; this would circumvent the principle of purpose limitation, and would therefore be from the outset impermissible. What the legislature intends to provide is only a limited facilitation of information transfer. This transfer of information is to leave the various agencies' rules on transfers in force, and its subject matter is to remain restricted to combating international terrorism. Although the term "terrorism" is not unambiguous in itself, the Counter-Terrorism Database Act uses § 129a of the Criminal Code as guidance; this derives from § 2 sentence 1 no. 1a ATDG – the central provision concerning the persons included in the database. "Terrorism", in this context, thus means specifically defined, serious criminal offences directed at the intimidation of the public or against the fundamental structures of a state or of an international organisation. This does not raise any constitutional objections. 106

2. The challenged provisions are also suitable and necessary to achieve this purpose. The data storage obligations under §§ 1 to 4 ATDG create a basic data inventory that is made available to the participating authorities pursuant to § 5 sec. 1, § 6 sec. 1 sentence 1 ATDG so that they can prepare further requests for information, and that is intended to provide them with information to protect against specific threats in particularly urgent cases, under § 5 sec. 2, § 6 sec. 2 ATDG. No other set of instruments that ensures these goals with comparable efficacy and less interference with rights is evident. 107

3. In its fundamental design, the Counter-Terrorism Database Act is also compatible with the principle of proportionality in the narrow sense. 108

The principle of proportionality in the narrow sense requires that in an overall as- 109

sessment, the severity of legislative restrictions on fundamental rights must not be disproportionate to the significance of the reasons that provide the justification for such restrictions. Here a fair balance must be established between the severity of interference with rights under the provision, and the intended legislative goal; between the individual interest and the public interest (cf. BVerfGE 100, 313 <375 and 376>; 113, 348 <382>; 120, 378 <428>; established case-law).

The severity of the challenged provisions' interference is substantial (a). This, however, is counterbalanced by significant public interests (b). A balancing does not lead to fundamental constitutional objections to establishing the counter-terrorism database, or to its nature; however, for the more detailed structuring of the database, clear legal provisions establishing adequate limits are necessary, including provisions for the effective supervision of its application (c). 110

a) The transfer of information created by the challenged provisions is of considerable severity. […] 111

aa) The severity of the interference by the counter-terrorism database is increased by the fact that it permits an exchange of information among a large number of security agencies, some of whose tasks and competences differ considerably from one another. It is particularly significant here that it also includes the transfer of information between intelligence services and the police. 112

(1) The authorisations for data collection and data processing conferred on each of the various security agencies are, so far as personal data are concerned, tailored to, and limited by, those agencies' specific tasks. Accordingly, the data are constitutionally subject to purpose limitations with regard to their use, and cannot automatically be shared with other agencies. Thus, the organisation of the security agencies according to their fields of specialisation and federal considerations also takes on a special dimension relating to fundamental rights where data privacy is concerned. The fact that information cannot be exchanged comprehensively and freely among the various security agencies is not an indication that these agencies are organised inappropriately for fulfilling their tasks, but is, as a general rule, prescribed and intended by the Constitution under the principle of purpose limitation pursuant to the data privacy laws. 113

However, the constitutional principle of purpose limitation for data does not preclude the possibility that the legislature may revise those purposes if such changes are justified by public interest concerns that override the constitutionally protected interests (cf. BVerfGE 100, 313 <360>; 109, 279 <375 and 376>; 110, 33 <69>). In assessing the proportionality of a transfer of information between different agencies, it is particularly important whether the different informational contexts are comparable. The more the agencies' tasks, authorities and manner of performing tasks differ from each other, the greater the significance of the transfer of related data. Therefore it is of particular significance for the constitutionality of such changes of purpose to what extent the limitations on data gathering by the transmitting agency, or in the present instance, 114

the agency entering data into the database, coincide with those under which the requesting authorities are allowed to collect data. Accordingly, a change of purpose is not allowed if it circumvents fundamental rights-based restrictions on the use of certain investigative methods, or in other words, if under the Constitution, the information could not have been legally collected either in this way, or at all, for the revised purpose, even if there had been a corresponding legislative basis (cf. BVerfGE 109, 279 <377>; 120, 351 <369>). […] Constitutional requirements for the gathering, storage and processing of data must not be circumvented by allowing agencies whose tasks place them under less rigorous standards to transmit data to agencies which, for their part, are subject to more rigorous standards.

(2) Accordingly, data pooling between the intelligence services and the police is of high significance and is, in general, subject to narrow constitutional constraints. This is because the police and intelligence services have tasks that differ sharply from one another. Accordingly, they are subject to fundamentally different requirements with respect to the openness with which they perform their tasks, as well as with respect to data collection. 115

(aa) The intelligence services have the task of gathering information even in advance of situations that pose a threat. […] 116

In keeping with this range of tasks that is performed in advance of such situations, the intelligence services have extensive data-gathering powers that are neither clearly defined with reference to specific areas of activity, nor particularly detailed as to the means to be applied. For the authorities for protecting the Constitution, they include methods and instruments for covertly procuring information, including the use of confidants and sources, observations, video and sound recordings, fictitious identification papers and fictitious vehicle number plates (cf. § 8 sec. 2 of the Federal Constitution Protection Act, *Bundesverfassungsschutzgesetz* – BVerfSchG; § 6 sec. 1 of the Baden-Württemberg *Land* Constitutional Protection Act, *Landesverfassungsschutzgesetz* – LVSG). Under § 5 of the Act Restricting Secrecy in Correspondence, the Mail, and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* – G 10, Article 10 Act), the Federal Intelligence Service may, in order to obtain information, and under certain circumstances, use strategic monitoring to filter international telecommunications connections for certain search criteria (cf. BVerfGE 100, 313 <368 et seq.> on the predecessor provision of the old § 3 sec. 1 G 10). Irrespective of the constitutional requirements, which are also differentiated here and are not concerned in the proceedings at hand, these powers reflect the breadth of tasks of the intelligence services, and are characterised by relatively low thresholds for interference. Furthermore, the intelligence services generally gather data covertly. The principle of openness in data collection does not apply to them, and they are largely exempted from obligations of transparency and reporting to the persons concerned. The options for individuals seeking protection of their rights are correspondingly meagre. In part they are even entirely superseded by political supervision (cf. Art. 10 sec. 2 sentence 2 GG). 117

By contrast, and to compensate for the breadth of these data collection powers, the goals at which intelligence activities may aim are limited. Without prejudice to more detailed differentiations among the various services, the goals are essentially limited to observing and reporting on fundamental threats that might destabilise the community as a whole, in order to permit a political assessment of the security situation. Not operational protection against threats is the goal, but providing political intelligence. For example, the task of the Federal Intelligence Service is not to combat criminal offences *per se*, but more generally to gather intelligence on foreign countries that is of importance for the foreign and security policy of the Federal Republic of Germany. In the form of situation reports, analyses and reports on individual findings, it is to enable the Federal Government to timely recognise threats, and to counter them politically (cf. BVerfGE 100, 313 <371>). Accordingly, intelligence gathering by the authorities for protecting the Constitution does not aim directly to avert and prevent specific criminal offences or to prepare corresponding operational measures. In this case, as well, the services' tasks are limited to a duty to report to the politically responsible state organs, or to the public, as the case may be (cf. BVerfGE 130, 151 <206>). 118

This task of the intelligence services, restricted to providing early political information, is also reflected in a restriction of the services' powers: they do not have police powers, and cannot ask the police, not even through inter-administrative assistance, to carry out measures for which they themselves have no authority. […] 119

(bb) The profile of tasks and powers of the law enforcement authorities and security agencies differs fundamentally from this profile. These entities have the responsibility of preventing, impeding and prosecuting criminal offences, and of protecting against other threats to public security and public order. Their tasks are characterised by an operational responsibility, and in particular by the power to enforce measures against individuals, if necessary by force. At the same time, their tasks are circumscribed by law in a differentiated manner and supported by a wide range of powers with many gradations, both substantive and procedural ones. Even though these agencies also have certain tasks in advance of threats, their general powers to act against individuals are situation-specific; as a rule, there needs to be cause to suspect the perpetration of an offence, or a danger. This profile of tasks is also consistent with these agencies' powers to gather and process data. As these powers can ultimately be used to prepare and justify measures of compulsion up to and including interference with personal freedom, they are considerably more narrowly and more precisely defined by law than those of the intelligence services, and are quite diversely distinguished from one another. Accordingly, and with numerous gradations in detail, these powers on the handling of data also require the existence of a specific cause such as a danger or the suspicion of an offence. If the legislature allows, as an exception, for personal data to be collected without a specific cause as a precaution or merely to prevent threats or criminal offences, this is in particular need of justification, and is subject to heightened constitutional requirements (cf. BVerfGE 125, 260 <318 et seq., 325 et seq.>). 120

Accordingly, the police normally act in the open, and likewise, their handing of data predominantly complies with the principle of openness. It is true that to a considerable degree, the tasks of the police also involve investigations that are initially conducted covertly against the person concerned. However, this exception applies only to certain information-gathering measures or phases that are supported by specific suspicions, and it does not alter the fact that police work is in principle conducted in the open. […] 121

The legal order therefore distinguishes between the police, which generally work in the open, are structured for the fulfilment of operational tasks, and guided by detailed legal provisions; and the intelligence services, which generally work in secret, are limited to observation and information gathering for political information and consultation, and can thus act within a less complex legal framework. No provision is made for a secret police. 122

(cc) In light of these differences, provisions that make it possible to transfer data between the police and intelligence services are subject to heightened constitutional requirements. From the fundamental right to informational self-determination follows a principle of separation of information (*informationelles Trennungsprinzip*). Under this principle, data may generally not be exchanged between the intelligence services and the police. The separation of data may be relaxed only by exception. If exceptions are granted for operational tasks, they constitute a particularly serious interference. Transfers of data between the intelligence services and the police for use in potential operational actions must therefore normally serve a particularly important public interest which justifies the access to information under the laxer requirements that apply to the intelligence services. This must be ensured by sufficiently specific and qualified thresholds for interference based on clearly defined legal provisions; moreover, the thresholds for the interference with rights in the acquisition of data must not be circumvented. 123

bb) However, it mitigates the severity of the interference that the counter-terrorism database is structured as a joint database which is essentially limited to facilitating access to information, and stipulates that the data may be used for operational tasks only in urgent and exceptional cases. 124

(1) The challenged provisions design the counter-terrorism database as a set of instruments that – except in emergencies under § 5 sec. 2 and § 6 sec. 2 ATDG – does not provide information so that the respective authorities can directly perform their tasks, and especially not their operational purposes, but provides it only as a basis for further data transfers. It is true that the counter-terrorism database itself enables a data transfer between the participating authorities by permitting searches of all basic data, and (as provided in § 5 sec. 1 sentences 1 and 2 ATDG) letting the requesting authorities have access to the simple basic data under § 3 sec. 1 no. 1a ATDG. However, § 6 sec. 1 sentence 1 ATDG provides that the requesting authority may use these data only for reviewing whether the data match the person being sought, and 125

for requesting the transfer of findings so that it can perform its own tasks. The information thus obtained, therefore, may normally be used only to decide whether to seek further information, and from what agency, and to provide better reasons for such individual requests for data transfers. In contrast to this, in case of specific requests, and thus also when operational tasks are performed, the transfer of data from the databases maintained by the various agencies is controlled by their relevant specialised law. Therefore, with regard to the simple basic data under § 3 sec. 1 no. 1a ATDG, the counter-terrorism database does not authorise an exchange of information so that certain tasks can be performed, but only prepares such an exchange. This applies even more to the extended basic data under § 3 sec. 1 no. 1b ATDG, which, as a rule, the authorities may access only as provided by the transfer provisions governing their particular agency (§ 5 sec. 1 sentence 4 ATDG).

126 Consequently, the Counter-Terrorism Database Act relies heavily on each agency's legal bases for data transfers, from which it derives its legal limitations. As a result, it ensures that – aside from cases under § 5 sec. 2, § 6 sec. 2 ATDG – an exchange of data for direct use in investigating and combating international terrorism is permissible only subject to the legal requirements of the transfer provisions for each of the agencies. It therefore balances the low requirements for initiating the receipt of information in advance of a threat – basically the question of necessity – with differentiated limits for the transfer of data. These restrictions must in turn meet the constitutional requirements and cannot be limited – at least not for data transfers between the intelligence services and the police – to comparatively minor requirements such as the data transfer being necessary for performing certain tasks or for preserving public safety.

127 (2) The function of the counter-terrorism database, which is essentially limited to facilitating access to information, significantly reduces the severity of its interference; nevertheless, even in this function, the severity of interference is still considerable. […]

128 Being included in such a database can represent a substantial hardship for the persons concerned. Once somebody has been included in the database, this person must expect, in the event of a search, to be categorised as affiliated with terrorism and – through further investigative requests thus facilitated – to be subjected to associated burdensome measures. The consequences of such a categorisation can be substantial, and they can place individuals in difficult situations without their knowing about the categorisation or having any practical way of defending themselves against it. The significance of this interference is intensified by the fact that the data are recorded in the database in isolation from their respective specific backgrounds, and may in part be founded on mere prognoses and subjective assessments by the authorities, which are uncertain by their very nature. Ultimately, citizens may thereby be exposed to considerable adverse consequences without having given any cause for which they themselves are accountable. It is true that in general, burdensome measures cannot be based directly on a use of the data in the counter-terrorism database

under the challenged provisions alone; instead, such measures loom as their indirect effect in conjunction with further provisions. The fact remains, however, that the counter-terrorism database increases the probability of such measures.

(3) The counter-terrorism database takes on a particular severity of interference to the extent that in emergencies, it also permits a transfer of information between intelligence services and the police in which the information may be used directly to defend against specific threats, and therefore also for operational purposes. 129

b) The establishment of the counter-terrorism database is, in general, compatible with the prohibition of disproportionate measures. The severity of the interference for the persons concerned is countered by the public interest in allowing, when investigating and combating international terrorism, a selective exchange of information between the various security agencies, and more accurate assessments in order to defend against the threat in important emergencies. 130

The legislature may attribute significant importance to establishing a central joint database in order to selectively exchange information for investigating and combating international terrorism. If only because of the number of agencies engaged in these tasks, ensuring an expedient exchange of findings among them is of particular significance. […] 131

Preventing and prosecuting terrorist offences that are organised internationally and committed in order to propagate fear and terror poses particular challenges for the governmental authorities who are responsible for that task. Because such offences are especially difficult to detect, and the target persons often act in a highly conspiratorial manner, the security agencies' success in effectively performing their tasks depends especially on the possibility that important information held by one agency can also be accessed by other agencies, and become meaningful information and provide meaningful overviews of a situation through pooling and matching of the various data from diffuse individual findings. It is obvious that a specially structured database that includes basic profiles of persons who have come to the authorities' attention, together with indications of which agencies can provide information about a given person, can significantly improve the performance of the authorities' tasks. It is also sound to assume that in serious emergencies, the authorities must have direct access to certain information from other authorities in order to be able to perform a first assessment of the threat and thus to permit appropriate further measures. 132

The great importance that effectively combating terrorism has for a democratic and free society must be taken into account in assessing the significance of such a database. Crimes with terrorist characteristics, at which the Counter-Terrorism Database Act is directed (see D. III. 1. above), aim to destabilise the community, and in so doing encompass attacks on the life and limb of random third parties, in a ruthless instrumentalisation of other human beings. They are directed against the keystones of the constitutional order and the community as a whole. It is a requirement of our constitutional order not to view such attacks as acts of war or states of emergency, which 133

would be exempt from adherence to constitutional requirements, but to fight them as criminal acts with means that are within the rule of law. This means, on the other hand, that within the constitutional examination of proportionality, the fight against terrorism must be accorded considerable weight (cf. BVerfGE 115, 320 <357 and 358>).

c) In view of the conflicting interests, an overall assessment shows no constitutional objections against the fundamental design of the counter-terrorism database as an instrument for initiating the receipt of information and as a source of information for initiating action when assessing threats in serious emergencies. However, the provisions for the database only meet the requirements of the principle of proportionality in the narrow sense if these norms are unambiguous and sufficiently narrow in defining which data are to be recorded and how these data may be used, and are in fact sufficiently limited, and if qualified requirements for supervision both exist and are adhered to (BVerfGE 125, 260 <325>). 134

[…] 135-137

IV.

On the basis of these principles, the challenged provisions do not meet the requirements for a structure of the counter-terrorism database that is sufficiently specific and complies with the prohibition of disproportionate measures in a number of ways. They violate the right to informational self-determination. 138

1. The provision under § 1 sec. 2 ATDG for involving further law enforcement agencies in the counter-terrorism database is incompatible with the requirement of specificity. 139

a) The principle of specificity aims to ensure that the law provides the government and administration with standards that guide and limit their actions, and that the courts can perform effective legal supervision. Specificity and unambiguity of the law also enable the citizens concerned to adjust to potential burdensome measures (cf. BVerfGE 110, 33 <52 et seq.>; 113, 348 <375 et seq.>; 120, 378 <407 and 408>). If the legislature itself specifies the cause, purpose, and scope of such measures, it may in some cases delegate their more detailed specification to the executive under Art. 80 sec. 1 GG, which must then specify them in regulations. […] The principle of specificity is therefore closely related to the constitutional reservations under which interferences with fundamental rights may be restricted only by legislation and, if applicable, on the basis of a law. […] The requirements for the specificity of legal provisions depend on the intensity of the interference with fundamental rights caused by the provision or arising on the basis of the provision. 140

According to these standards, the authorities participating in the counter-terrorism database must be defined either directly by legislation, or by a regulation based on legislation. The decision as to which authorities must submit their data to the database, and which ones may consult the data, significantly defines the scope and content of the database as well as the scope of the further use of the data. This is an es- 141

sential regulatory element that requires an unambiguous, specific definition which has an external effect. […]

b) Neither in itself nor in conjunction with the order to open a data file under § 12 ATDG does § 1 sec. 2 ATDG satisfy the special requirements that must be met in the legal specification of the participation of further law enforcement agencies in the counter-terrorism database. 142

aa) By itself, § 1 sec. 2 ATDG does not provide a sufficiently unambiguous legal definition from which the participating authorities can be determined directly. It is true that the requirements for specificity do not *per se* exclude the legislature's option to define the agencies authorised to use a database only generally and in the abstract, depending on the database's nature and purpose. If the set of these agencies can be determined with sufficient specificity directly from the law, it may do no harm if the individual agencies are not mentioned expressly (cf. BVerfGE 130, 151 <199, 203>). But that is not the case here. § 1 sec. 2 ATDG describes the participating agencies only in terms of broad criteria that require discretionary judgment. […] 143

bb) Nor does a sufficiently clear specification of the participating agencies proceed from § 1 sec. 2 ATDG in conjunction with the order to open a data file under § 12 no. 2 ATDG. There are no general objections to delegating the final determination of these authorities to the executive branch. However, since defining the agencies that participate in the counter-terrorism database is of specific relevance to fundamental rights, it is not sufficient to draft an order to open a data file as a mere administrative rule that has no legally binding effect on the persons whose data are affected or on the courts, and that also is not issued and promulgated as a law or regulation. If the legislature chooses to place the decision about the participating agencies in the hands of the executive, Art. 80 sec. 1 GG requires it to do so in the form of a regulation. 144

2. Not in every respect compatible with the constitutional requirements are the provisions which determine the group of persons who the database may cover. Some of these provisions violate the principle of specificity and the prohibition of disproportionate measures. Others are in need of an interpretation to narrow them in conformity with the Constitution. 145

a) However, there are no objections to § 2 sentence 1 no. 1a ATDG. This provision requires data about persons who may belong to or support a terrorist organisation to be collected, and therefore covers those who are the focus of an effective defence against terrorism. Since this provision is linked to provisions of criminal law that criminalise certain activities long before legally protected interests are actually violated, and since it only requires "factual indications" – if applicable, even for support actions – this clause indeed gives the authorities substantial leeway for subjective assessments, and it is subject to many other uncertainties. However, this structure is acceptable in the context of the counter-terrorism database, which (apart from serious emergencies) only serves to initiate the receipt of information, and which, in that context, is 146

meant to make it possible to reject or confirm uncertain assessments of suspicious or threatening situations even before investigations have taken place. If properly interpreted, these constituent elements still provide an adequate assurance that data may not be stored on the basis of mere speculation. […]

b) § 2 sentence 1 no. 1b ATDG, which expands the group of included persons from the viewpoint of support for terrorist organisations, is in part not compatible with the prohibition of disproportionate measures and is unconstitutional. 147

aa) However, the provision is unobjectionable to the extent that it includes persons who belong to a group that supports a terrorist organisation. […] 148

bb) By contrast, that group is expanded further in that the provision also includes persons who merely support a supporting organisation. No requirement for a subjective connection to terrorism can be found in the provision. According to its wording and an object and purpose that is not unlikely, the provision thus also covers an extension of the data storage obligation to persons who, far prior to any terrorism, and possibly without knowing of any connection with terrorism, support what they believe to be an innocuous organisation, such as the kindergarten of a mosque association, while the authorities suspect this association of supporting terrorist organisations. Such a broadening of the law to include even the remotest connections with terrorist organisations violates the principle of unambiguity of legal provisions, and is incompatible with the prohibition of disproportionate measures. Of course, the legislature is free to view the mere support for supporting organisations as a reason for data to be stored, if there are factual indications that this support is a deliberate encouragement of those activities of such groups that support terrorism. However, in that event, the legislature must express this in such a way in the law that the principle of unambiguity of legal provisions is observed. […] 149

c) § 2 sentence 1 no. 2 ATDG is not fully compatible with the Constitution. This provision, which is meant to cover individuals who might have an affinity to terrorism, combines a number of ambiguous and potentially broad legal terms. Because of a tie in the Senate's votes, the terms "unlawful use of violence" ("*rechtswidrige Gewalt")* and "intentional incitement of such use of violence" ("*vorsätzliches Hervorrufen solcher Gewalt")* cannot be declared unconstitutional. In the opinion of the four members of the Senate who carry this part of the decision (§ 15 sec. 4 sentence 3 BVerfGG), the use of these criteria is compatible with the Basic Law as long as they are not accorded an overly broad meaning (aa). In the opinion of the other four members of the Senate, which ultimately does not prevail for this decision (§ 15 sec. 4 sentence 3 BVerfGG), the provision would have to be declared unconstitutional in this regard (bb). However, in the unanimous view of the Court, the mere "advocacy" ("*Befürworten")* of violence within the meaning of this provision is not sufficient for recording a person in the counter-terrorism database. To that extent, the provision violates the prohibition of disproportionate measures and is unconstitutional (cc). 150

aa) (1) The provision focuses mainly on the notion of unlawful use of violence. This 151

term has a very broad meaning in other parts of the legal system, which would not be significant enough to serve as an indication that the persons concerned have an affinity with terrorism. It could not narrow down the group of persons concerned in a manner that suffices for the principle of proportionality, and that could establish constitutional support for storing their data. […] In accordance with the objective of the counter-terrorism database, which is directed against terrorist criminal acts, this term must instead be understood as covering only violence directed immediately against life and limb, or characterised by the use of means that pose a danger to the public. Under this interpretation, there are no constitutional objections to the proportionality of the group of persons covered by using the term “violence” in § 2 sentence 1 no. 2 ATDG.

(2) Furthermore, § 2 sentence 1 no. 2 ATDG includes both persons who use, support and prepare violence, and those who merely advocate it or who intentionally incite it. This would open up disproportionately broad possibilities for interference if even conditional intent (*Eventualvorsatz*), as used in the terminology of criminal law, were viewed as sufficient for the intentional incitement of violence. However, if, in this context, the criterion of intentional incitement of violence is attributed a meaning whereby only the deliberate incitement of violence is covered, this complies with the principle of proportionality. 152

bb) In the opinion of the other four members of the Senate, which ultimately does not prevail for the decision (§ 15 sec. 4 sentence 3 BVerfGG), § 2 sentence 1 no. 2 ATDG must be declared entirely unconstitutional because of lack of specificity and its overly broad reach. This cannot be cured by assuming a narrower interpretation of the terms “unlawful use of violence” and “intentional incitement” that diverges from the notions generally used in criminal law. Such a recourse to an interpretation in conformity with the Constitution is inconsistent, and relaxes the requirements for specificity under data privacy law. 153

(1) As also the members of the Court whose position prevails see, significant criteria of this provision are ambiguous, and are elsewhere in the legal system – specifically, in an area of criminal law that is fundamental to everyday legal concepts – interpreted broadly and in a manner that is, in the context of the counter-terrorism database, incompatible with the requirements of proportionality and the prohibition of disproportionate measures. […] 154

(2) There is no possibility of a narrower interpretation in conformity with the Constitution. 155

(a) Such an interpretation is not possible for § 2 sentence 1 no. 2 ATDG, if only because the term “unlawful violence” that is central to the provision was intentionally chosen by the legislature to be broad and open. The vagueness and overly wide reach of the concept of violence were explicitly criticised in the legislative process (Plenary Minutes of the Bundestag – BTPlenarprotokoll *16/71, p. 7100; Bundestag Committee on Internal Affairs, Minutes no. 16/24, p. 55; Committee Document – A-* 156

Drucks 16(4)131 D, p. 10; A-Drucks 16(4)131 J, p. 10). Even a particular counter-proposal submitted to restrict it, under which, on the basis of § 129a sec. 2 StGB, unlawful violence was to serve as a connecting factor for data storage only "if [unlawful violence] is intended to intimidate the population in a significant manner, to unlawfully coerce an authority or international organisation, or to eliminate or significantly impair the fundamental political, constitutional, economic or social structures of a state or international organisation, and the person's actions threaten to significantly damage a state or an international organisation" (cf. BTDrucks 16/3642, pp. 14 and 15). An attempt was thereby made to narrow the concept of violence similarly to what is also being striven for in international and European provisions for combating terrorism (cf. Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164/3 of 22 June 2002, Art. 1; Draft of a General 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.). The legislature, however, made a deliberate decision to ignore this proposal – obviously in order to give broader latitude to the security agencies. Such a decision cannot be cured by way of an interpretation in conformity with the Constitution.

(b) However, an interpretation in conformity with the Constitution is also not possible because of considerations of principle. If the statutory basis for interference is worded openly in the aforementioned manner, and – as is not far-fetched – if it also supports such an overreaching interpretation when recognised definitions are used, it does not comply with the principle of unambiguity of legal provisions and is disproportionate as a foundation for data processing such as is under discussion here. The principle of unambiguity of legal provisions specifically aims to demand from the legislature itself sufficiently clear decisions regarding the requirements for interferences with fundamental rights, so as to uphold the prohibition of disproportionate measures with sufficient reliability. If the legislature fails to meet these requirements, the Federal Constitutional Court cannot cure the deficiency with an interpretation in conformity with the Constitution. […] 157

The requirements for specificity and for a sufficiently clear limitation of the legal foundations differ depending on the subject matter and the regulatory context. According to the established case-law of the Federal Constitutional Court, the requirements for specificity and unambiguity of legal provisions are especially rigorous in data privacy law (cf. BVerfGE 65, 1 <46>; 118, 168 <187>; 120, 378 <408>) – and this must especially apply to the counter-terrorism database, which governs the exchange of data among security agencies even in advance of investigations. Unlike in the enforcement of laws (for example through an executive action) where official measures are directed against an individual, are provided with reasons, and can be reviewed by a court in the individual case, data processing under the Counter-Terrorism Database Act takes place out of reach of any direct view. It remains informal, the person concerned is given no reasons, and it generally can also not be reviewed by a court. […] 158

These qualified requirements for specificity in constitutional data privacy are also not founded on an exaggerated mistrust of the security agencies. Rather, such requirements shall in themselves ensure unambiguous conditions that provide the authorities with the clearest possible guidance in performing their demanding tasks, and also relieve them in case of doubt, especially when performing the security agencies' tasks which are not yet or only loosely formalised and where data processing often plays a special role. 159

(c) Nor is an interpretation in conformity with the Constitution required out of respect for the legislature. It is true, that with the Counter-Terrorism Database Act, the legislature created an ambitious and nuanced regulatory concept which in many regards is characterised by moderation under the rule of law and by a serious effort to guarantee appropriate data privacy. However, a constitutional assessment of the actual provisions that implement this concept cannot be guided by an overall assessment of the legislature's political efforts. Rather, it is the court's task to apply the constitutional standards independently from such considerations, and in detail, and thereby to ensure that the rule of law that forms a basis for the overall design does not slip away through loopholes in individual provisions. […] 160

cc) The criterion of "advocacy of violence" has an especially broad reach. Here the legislature only refers to an internal attitude that need not have resulted in any activity that encourages violence. The use of this criterion is incompatible with the Constitution, and the provision is unconstitutional to that extent. The generally overly wide reach of this criterion can also not be remedied through an interpretation in conformity with the Constitution. […] Linking to such a criterion, which focuses directly on the *forum internum* and therefore interferes with an individual's inaccessible inner sphere, is particularly capable to also have an intimidating effect on the exercise of legal freedoms, particularly the freedom of religion and the freedom of expression. In this case, the law uses subjective convictions *per se* as its yardstick and thus lays out criteria that an individual can only control to a limited degree and that cannot be influenced by law-abiding conduct. Including persons in the counter-terrorism database on the basis of such a criterion is incompatible with the prohibition of disproportionate measures. § 2 sentence 1 no. 2 ATDG is unconstitutional to that extent. 161

d) § 2 sentence 1 no. 3 ATDG is also unconstitutional. The inclusion of contact persons it provides for is incompatible with both the principle of specificity and the prohibition of disproportionate measures. 162

§ 2 sentence 1 no. 3 ATDG provides that even mere contact persons of the persons covered by the preceding clauses must be included in the counter-terrorism database. The law treats these as a separate group, whose data are made accessible to the participating authorities in the same way as those of the other persons included in the database. Also to be included in the database are those contact persons who know nothing about the principal's connection with terrorism – although in this case only their simple basic data are to be included (§ 3 sec. 1 no. 1a ATDG). If these are 163

contact persons who know of the relevant principal's connection with terrorism, the extended basic data (§ 3 sec. 1 no. 1b ATDG) are also to be entered in the database.

The provision that includes contact persons as a separate group in a data transfer that also incorporates unmasked information does not meet the requirements for specificity. On this basis one cannot predict which persons are in fact to be included in the database. Even if the legislature makes an exception for persons who have only a fleeting or chance contact, the provision includes everyone throughout the social living environment of the persons named under numbers 1 and 2 of the provision – both those in the private environment and those who have professional or business contacts with them. But evidently not all persons who thus come under consideration are actually supposed to be included in the database. […] Rather, the determination of what data are to be stored is ultimately left up to [the authorities'] free discretion. 164

In view of the size of the group of persons covered by the provision, which is scarcely comprehensible, the provision also violates the prohibition of disproportionate measures. However, it is not generally prohibited by constitutional law to make data of contact persons available in the counter-terrorism database. As a rule, such persons who are not covered by numbers 1 and 2 of the provision, and who therefore do not themselves count as potential supporters of terrorist activities, are, according to the database's purpose, only of interest to the degree they can provide information about the principal who is thought to have a close connection to terrorism. The design of the legislation must take its guidance from this fact. […] This applies irrespective of whether such contact persons do or do not know about the principal's connection with terrorism. 165

3. There is no constitutional objection to the scope of data collected, as provided under § 3 sec. 1 nos. 1a and 1b ATDG. However, with regard to § 3 sec. 1 no. 1b ATDG, which already includes some requirements for further specification by the administration, supplementary provisions are needed. 166

a) The specification of the basic data described under § 3 sec. 1 no. 1a ATDG and made available to the participating authorities as unmasked information without qualified thresholds for interference is not constitutionally objectionable. 167

However, the scope and significance of these data are considerable. […] 168

Nevertheless, the provision is compatible with the prohibition of disproportionate measures. The description of the data is sufficiently specific, and its reach is proportionate, even in an overall assessment. Limited to persons who may be potentially affiliated with terrorism (see D. IV. 2. above), the data are used in preparing a meaningful basic profile for the more precise identification of the persons concerned. That profile, however, is ultimately still limited to external parameters. In view of the importance of combating terrorism, this is constitutionally unobjectionable even if one includes the data from the intelligence services. Here it must again be borne in mind that these data are not gathered anew, and therefore the database does not aim for 169

the investigative preparation of a profile with a full set of basic data, but merely brings about a pooling of the data already held by the individual agencies. […]

b) There are also no constitutional objections in terms of the prohibition of disproportionate measures with regard to the scope of the extended basic data to be stored under § 3 sec. 1 no. 1b ATDG; these are normally provided to the participating agencies only indirectly after a search resulted in a match, and are released directly only in emergencies. However, the legislature must ensure that the specifications governing application are comprehensibly documented and published for those criteria whose content will be defined only by a further abstract and general specification by the administration. 170

aa) The storage of the criteria under § 3 sec. 1 no. 1b aa to ff, jj, ll, mm, oo, pp and qq ATDG is constitutionally unobjectionable. 171

(1) The criteria to be entered in the counter-terrorism database under these provisions are defined with sufficient specificity by the legislature, and do not rely on the intermediate step of an abstract and general specification by the executive. The scope of the obligation to store data is directly evident from them, and their application can readily be reviewed in audits by supervisory entities and, if applicable, examinations by the courts. […] 172

(2) The criteria to be recorded according to these provisions are also in terms of their scope and significant content compatible with the prohibition of disproportionate measures. 173

However, the potential significance of these data is extensive. […] 174

On the other hand, here too it must be taken into account that the provisions do not provide for the collection of new data, but only for a pooling of the data already held by the individual agencies. Most importantly, however, this severity of interference is countered by the highly important public interest in the effective investigation and combating of international terrorism (see above, D. III. 3. b) […]. 175

This applies first of all to the aim of being able to provide these data directly and in full in emergencies for an initial assessment of a threat, so as to guide further action. […] 176

But it also applies to the further purpose pursued in storing these data: their indirect, qualified use for initiating the receipt of information. Precisely because the investigative possibilities opened up by the content of these data are far-reaching, they can make investigations to avert terrorism significantly more expedient, and there is an important public interest in having the data made available. Because the data remain limited to a group of persons affiliated with terrorism, and to data that have already been gathered, there is, in principle, no objection to their being made available. The crucial factor for extended basic data here is that they are provided only indirectly subject to a specific request process to the authorities to initiate the receipt of infor- 177

mation, but are transmitted directly only as provided by the particular laws in this area. […]

bb) The storage of the criteria under § 3 sec. 1 no. 1b gg, hh, ii, kk, nn ATDG is also compatible with the Constitution. For these criteria, however, the legislature must ensure that the specific rules necessary for their application by the administration are documented and published. 178

(1) The provisions comply with the principle of specificity. 179

However, these provisions are particularly in need of practical specification, and do not completely indicate to the citizen what information is actually included in the database. For example, the range of special skills for preparing and carrying out terrorist acts, or of employment in official buildings, or of places or regions where persons affiliated with terrorism meet, is extraordinarily broad. Moreover, it would be difficult to assess on the basis of the law alone what should be recorded about ethnic origin or religious affiliation, in view of the differently nuanced options for practical specification. Also according to the legislative intent, the detailed specification of the information to be included in the database was not to be conclusively covered in the provisions of the law itself, but only in further abstract and general practical specifications laid down by the security agencies, who must define these, in a first phase, via an order under § 12 no. 3 ATDG, and ultimately in a standardised computer program (cf. BT-Drucks 16/2950, p. 17). Irrespective of setting up § 3 sec. 1 ATDG as a strict data storage obligation, the legislature evidently did not wish to conclusively decide in these provisions that all information that might fall under the characterising features named here were in fact to be incorporated into the database. Rather, this is to be decided by the agencies. 180

Despite this open-endedness and need for further specification, in the overall context of the database these provisions comply with the requirements for unambiguity of legal provisions and the principle of specificity. The principle of specificity does not automatically forbid the use of vague terms of law (BVerfGE 118, 168 <188>). However, the legislature must draft its laws as specifically as possible in view of the particular nature of the matters to be governed, giving consideration to the purpose of the law (BVerfGE 78, 205 <212>; cf. also BVerfGE 110, 370 <396>; 117, 71 <111>). It must be possible to adequately concretise vague terms of law by an interpretation of the relevant provisions according to the rules of legal methodology, and any remaining uncertainties must not be so extensive as to jeopardise the predictability and judicial reviewability of the acts of the government agencies empowered by the provisions (cf. BVerfGE 21, 73 <79 and 80>; 118, 168 <188>; 120, 274 <316>; established case-law). 181

In the context of the counter-terrorism database, which primarily initiates the receipt of information among diverse security agencies, and which aims at facilitating the use of dispersed and even unverified findings by other agencies in order to render the protection against terrorism more effective, a more precise legislative description of 182

the data to be stored cannot reasonably be demanded. Which aspects may be significant for investigations in the individual case is closely related to the authorities' level of knowledge, may change at short notice because of unforeseen events, and may then require rapid updating. Thus the final limitation of the relevant criteria is possible only on the basis of specific specialised understanding and current assessments. Under these circumstances, it is not objectionable from the viewpoint of specificity if the legislature provides an open-ended description of the data to be stored which is still in need of practical specification, and if the legislature prescribes a tiered procedure for their specification while using them, a procedure in which the information actually to be entered into the database is further specified and limited according to professional expertise. Such a specification, even if it includes abstract and general determinations that are of considerable importance, is not a task that is necessarily incumbent upon the legislature itself. Rather, in a state with a separation of powers, it may without constitutional objections be entrusted to the executive. The defining factor is that in the present case, the legislature has not granted a blanket authorisation to the authorities, but has described the criteria in such a way that those criteria can be defined further. The aspects and focus of the data to be stored are legislated in their content, and supported with examples and assessment criteria, in such a way that they are meaningful as a foundation for a further specification by the executive, and contain clear guidelines and limits for that purpose. Here again one must keep in mind that this concerns only the specification of the scope of those data that are already held by the entering authorities, that are to be included in the database, and that concern persons who could be viewed as possibly affiliated with terrorism; the group of those persons must be described with sufficient limitations by the legislature itself (see D. IV. 2. above).

(2) To compensate for the open-endedness and need for further specification of these provisions, the legislature must ensure that the specification and standardisation that will ultimately govern the application of the provisions in an individual case are comprehensibly documented and published by the security agencies. 183

[…] Such a definition, documentation and disclosure serves, first of all, to circumscribe the authority granted to the executive by forestalling an overreaching or abusive application of the provision (cf. Constitutional Court of the Free State of Saxony, *Verfassungsgerichtshof des Freistaates Sachsen* – SächsVerfGH, [judgment of 10 July 2003 – Vf. 43-II-00 –, juris,] para. 198). Second, it ensures an adequate level of supervision. The documentation and disclosure of the criteria defined by the executive will in particular enable the Data Privacy Commissioners to monitor whether the application of the provisions by the executive, which the legislature conceived to evolve in stages, follows rational criteria and is guided by the intent and purpose of the law. 184

The current legal status does not fully meet these requirements […]. 185-186

[…] If the legislature intends to adhere to the vague terms of law in § 3 sec. 1 no. 1b 187

gg, hh, ii, kk, nn ATDG, a supplementary provision is necessary that ensures an understandable documentation and publication of the specification of these criteria, which the legislature intended, by the security agencies .

(3) The criteria to be included in the database under § 3 sec. 1 no. 1b gg, hh, ii, kk, nn ATDG are in their content compatible with the prohibition of disproportionate measures. Although these are data which – especially in conjunction with the other criteria to be stored – may in some cases reveal highly personal facts, in view of the limiting function of the database and the significance of the protection against terrorism (cf. D. III. 3. a) bb), b above), the legislature is operating here within the discretionary margin to which it is entitled. 188

This also applies to the criteria of ethnic origin and religious affiliation under § 3 sec. 1 no. 1b gg and hh ATDG. However, particularly stringent requirements apply to recording these criteria, because they are covered by a special constitutional protection against discrimination under Art. 3 sec. 3 GG, and religious affiliation is specially protected from an obligation to disclose by Art. 140 GG and Art. 136 sec. 3 of the Weimar Constitution (*Weimarer Reichsverfassung* – WRV). Accordingly, these data are also deemed especially sensitive in other contexts (cf. § 3 sec. 9, § 28 secs. 6 to 9 of the Federal Data Privacy Act (*Bundesdatenschutzgesetz* – BDSG), Art. 8 sec. 1 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and Art. 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 [BGBl 1985 II p. 539]). However, in view of the importance of an effective defence against terrorism, it is not completely impossible to consider these data, too. Nevertheless, the Constitution requires that their consideration be restrained. This must be taken into account by ensuring that such information can only be recorded for identification purposes. 189

cc) The free text field under § 3 sec. 1 no. 1b rr ATDG is also compatible with the prohibition of disproportionate measures. This is not a blanket authorisation for adding further information to the database at will, but opens the database for notes and assessments which cannot be shown otherwise due to the standardisation and catalogisation of the entries. […] 190

4. The provisions for the use of the data are not in every respect compatible with the prohibition of disproportionate measures. 191

a) However, the provisions on the request and use of the simple basic data under § 3 sec. 1 no. 1a ATDG are constitutionally unobjectionable. 192

aa) § 5 sec. 1 sentence 1 and 2 ATDG provide the participating agencies with direct access to these data as unmasked information. An agency can thus make searches both based on a name, and searches that relate to individual or multiple types of information listed in § 3 sec. 1 no. 1a ATDG, and which therefore help identify persons not 193

yet known to that agency. In the event of a match, access is then granted to the entire set of simple basic data stored for these persons. For this, § 5 sec. 1 sentence 1 ATDG does not establish qualified thresholds for interference. It is sufficient if a search is necessary in order to perform the relevant tasks for investigating or combating international terrorism. […]

Consequently the participating agencies have extensive room for searches in the basic data. But this does not mean that these authorisations are unlimited. One limit, in particular, consists in that § 5 ATDG permits only individual searches, but not screening, collective searches, or a generalised investigation of connections between persons by linking data fields. The provision therefore requires a specific cause for investigation. Moreover, every request is subject to the requirement of necessity, which must be duly examined in each case. Furthermore, the provision in its present form does not authorise either automatic image recognition or the use of “find-like” functions or searches with incomplete data (known as “wildcards”). 194

bb) Despite the remaining breadth of search possibilities, caused in particular by the absence of limiting thresholds for interference, the provision is compatible with the principle of proportionality. The defining factor for this are the rules governing use. Under § 6 sec. 1 sentence 1 ATDG, the transferred data may be used only to identify persons relevant to an investigation, and to prepare individual transfer requests to the authority holding the relevant information. The authorities are not permitted to derive any further information guiding investigations or actions from these data. They may only obtain that information in a further step as provided by the laws governing their agencies. […] With reference to the simple basic data under § 3 sec. 1a ATDG, such a transfer, limited to phases in advance of investigations, is unobjectionable from the viewpoint of proportionality, considering the great importance of protection against terrorism. To that extent, § 5 sec. 1 sentences 1 and 2, § 6 sec. 1 sentence 1 ATDG are constitutional. 195

b) The searches permitted under § 5 sec. 1 sentence 1 and 3 ATDG of extended basic data under § 3 sec. 1 no. 1b ATDG are also compatible with the prohibition of disproportionate measures, provided that those searches are carried out with reference to particular names. § 5 sec. 1 sentence 1 ATDG permits requests with regard to all data included in the counter-terrorism database, and therefore also searches of extended basic data. If a search for a personal name results in a match in the extended basic data, however, under § 5 sec. 1 sentence 3 ATDG the agency does not receive access to the extended basic data themselves, but only a match message, combined with the information about which agency maintains corresponding information including the file number. Access to the extended basic data themselves is only granted by individual request subject to the laws governing the particular agency, by way of a release on the part of the authority maintaining the information (§ 5 sec. 1 sentence 3 and 4 ATDG). […] 196-197

c) However, the authorisation of criteria-based searches of the extended basic data 198

that do not send the searching agency merely a reference to further information in the event of a match, but provide direct access to the corresponding simple basic data under § 3 sec. 1 no. 1a ATDG, is not compatible with the prohibition of disproportionate measures. To that extent, § 5 sec. 1 sentence 2 no. 1a ATDG is unconstitutional.

The informational content of the extended basic data under § 3 sec. 1 no. 1b ATDG is far-reaching, and can include highly personal information, as well as information that portrays the biography of the persons concerned (see D. IV. 3. b) aa) [2] above). From the viewpoint of proportionality, therefore, access to such information must be substantially more limited than is the case for the simple basic data under § 3 sec. 1 no. 1a ATDG. The legislature itself therefore provides in general only for an indirect search of these data, and makes their transfer as unmasked information subject to the transfer regulations that govern the agency concerned. But because, in searches of these data, the legislature also allows access to the simple basic data as unmasked information in the event of a match, it significantly retracts this restriction for criteria-based searches, i.e., “reverse searches”. By linking a match message for extended basic data with the individualised information in the simple basic data, the extended basic data searched also become individually attributable, and can be exploited as personal information. In this way, by searching for one or more criteria – for example, by searching for persons with a certain religious affiliation and qualification who frequent a certain meeting place (cf. § 3 sec. 1 no. 1b hh, jj, nn ATDG) – agencies can perform a search and obtain, in the event of a match, not just the information about which agency holds relevant information, but all names, addresses, and other information listed in § 3 sec. 1 no. 1a ATDG about everyone who matches the search criteria. 199

Such a far-reaching use does not take sufficient account of the significance of the content of the extended basic data. […] Accordingly, a provision for use must be designed in such a way that if a search also reaches into extended data, only the file number and the agency holding the information will be displayed, but not the corresponding simple basic data. 200

d) By contrast, there are no constitutional objections to the use of extended basic data in emergencies under § 5 sec. 2, § 6 sec. 2 ATDG, even in the case of a reverse search (cf. c above). 201

It is true that this is the broadest possible use of the data pooled in the counter-terrorism database. In addition to the simple basic data, use here also includes all extended data as unmasked information, and therefore opens the way not just for the use of data in the preparation of further investigative requests, but – as part of an assessment of a threat so as to guide further action – in defending against terrorism itself (§ 6 sec. 2 ATDG). Particularly because of the associated abrogation of the principle of separation of information between intelligence services and the police (*informationelles Trennungsprinzip*), this leads to an especially severe interference (see D. III. 3. a) aa), bb) [3] above). 202

The conditions under which such a use is permitted are, however, sufficiently narrowly defined to justify the interference. The data may be accessed and used only to protect especially significant legally protected interests – which means, first of all, to protect life, limb, health or freedom of human beings. […] Insofar as the provision additionally includes the protection of property of substantial value, the legislature makes clear that this does not pertain to the protection of ownership or property *per se*, but goods "the preservation of which is in the public interest" (§ 5 sec. 2 sentence 1 ATDG). This means, in the context of protection from terrorism, such property as significant infrastructure or other facilities of direct importance for the community. The provision also includes high thresholds for interference. The protected interests must be exposed to a present threat founded not just on factual indications, but on specific evidence. Here the data may be accessed and used only when this is indispensable and the requested data cannot be transferred in due time. Moreover, access to the data is procedurally safeguarded. […] 203

5. The principle of proportionality also sets requirements for transparency, protection of individual rights, and supervisory oversight. Due to the purpose and functioning of the database, the Counter-Terrorism Database Act ensures transparency of the exchange of information only to a limited extent. Thus, only limited possibilities of legal protection are open to the persons affected; the supervision of its application is carried out principally through oversight by the Data Privacy Commissioners. This is compatible with the Constitution if the conditions set out in constitutional law are adhered to when it comes to effectively organising the supervision. 204

a) For the storage and use of personal data in performing official tasks, the legislature must also comply with proportionality-related requirements for transparency, legal protection, and supervisory oversight (cf. BVerfGE 125, 260 <325 et seq.>). 205

[…] 206-207

b) The Counter-Terrorism Database Act contains few provisions for the establishment of transparency and for ensuring the protection of individual rights. In essence, it is limited to recognising rights to disclosure, which are of limited effectiveness both procedurally and in terms of content. In view of the function and manner of operation of this database, however, this is not objectionable. 208

aa) As a primary instrument for ensuring transparency, the Counter-Terrorism Database Act provides rights to information as provided in the Federal Data Privacy Act (§ 10 sec. 2 ATDG). These rights, of course, are subject to limitations, and to some extent may be exercised only with substantial procedural effort. However, in view of the function of the Counter-Terrorism Database Act, they suffice to meet the constitutional requirements. 209

[…] 210-212

bb) Otherwise, the Counter-Terrorism Database Act includes neither a principle for openness of data use, nor a reservation of certain matters for the jurisdiction of the 213

courts, nor its own duties of subsequent notification, that go beyond the duties of notification under other provisions. It therefore omits important instruments for ensuring proportionality of the rules governing database use. In view of the purpose of the counter-terrorism database, however, this is constitutionally justified. […]

c) Since transparency of data processing and enabling the protection of individual rights can be ensured only to a very limited degree by the Counter-Terrorism Database Act, guaranteeing effective supervisory oversight is all the more significant. Therefore, the principle of proportionality poses more rigorous requirements for the effective design of this supervision both at the level of the law itself and in administrative practice. 214

aa) Guaranteeing effective supervision first of all necessitates supervisory authorities equipped with effective powers at both the federal and *Land* level, such as the Data Privacy Commissioners under the current law. It is also necessary to keep full records of accesses to and modifications of the data inventory. In this regard, technical and organisational measures must ensure that the data are available to the Data Privacy Commissioners in such a way that they can be evaluated in a practicable manner, and that the records include sufficient information to match them with the process to be audited. 215

Given the nature of the counter-terrorism database as a joint database used both by the federal and *Land* authorities, it must be ensured that uncertainties about areas of federal responsibility do not cause the effective supervision of the database to take second place to providing effective data transfer. […] It must likewise be ensured that in the interaction among the various supervisory authorities, practicable and effective supervision of the data obtained under the Article 10 Act – which are of particular importance in a database to which also the Federal Intelligence Service contributes a significant amount of the content – is ensured. If the legislature provides for cooperation among security agencies in matters of information, it must also permit supervisory cooperation for the benefit of data privacy. 216

Since supervisory oversight has the function of compensating for the weak level of the protection of individual rights, regular supervision is particularly significant, and 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 in granting the associated powers. 217

bb) Guaranteeing compliance with the constitutional requirements for effective supervisory oversight is the joint responsibility of the legislature and the authorities. 218

[…] 219-220

d) […] 221

Since the storage and use of data under the Counter-Terrorism Database Act largely takes place hidden from the perception of the individuals concerned and the public, 222

and since rights to obtain information have only a limited counteracting effect and the courts have no adequate possibility for effective supervision, regular reports by the Federal Criminal Police Office to Parliament and the public on the contents and use of the counter-terrorism database must be ensured by law. […]

6. There are no constitutional objections to the provisions for deletion under § 11 sec. 2 and 4 ATDG. […] 223

V.

To the extent that the challenged provisions provide that data to be included in the counter-terrorism database may include data that are obtained by interferences with the secrecy of telecommunications or with the fundamental right to inviolability of the home, they violate Art. 10 sec. 1 and Art. 13 sec. 1 GG. 224

1. For the collection of data via interferences with the fundamental rights under Art. 10 sec. 1 and Art. 13 sec. 1 GG, especially strict requirements apply in view of the special protective content of those rights. According to the case-law of the Federal Constitutional Court, these stricter requirements also continue to apply in the requirements for the transfer and the alteration of the purpose of the data thus obtained. […] It is in accordance with this requirement that data that derive from serious interferences with Art. 10 sec. 1 or Art. 13 sec. 1 GG must be labelled. The recognisability of such data is intended to ensure that the specific limits on data use are obeyed even after the data may have been forwarded to other agencies. 225

2. A full, unrestricted inclusion in the counter-terrorism database of all data gathered by interferences with Art. 10 sec. 1 and Art. 13 sec. 1 GG is not compatible with these requirements; nor can anything else apply to data that are obtained by interfering with the fundamental right to a guarantee of confidentiality and integrity of information technology systems – of which the complainant does not complain – under Art. 2 sec. 1 in conjunction with Art. 1 sec. 1 GG (cf. BVerfGE 120, 274 <302 and 303>). Such data may generally be gathered only subject to strict standards, and require, for example, elevated thresholds for interference, such as an especially dangerous situation or a specific suspicion of an offence, a threat to especially significant legally protected interests, or the prosecution of especially serious criminal offences. […] 226

3. This is not altered by the Federal Government's statement at the oral hearing that in the future, in accordance with § 4 ATDG, such data will only be indirectly accessible in case of a match. No such restriction proceeds from the Counter-Terrorism Database Act. […] 227

However, a provision that always provides for covert storage of such data under § 4 ATDG would under proportionality aspects be compatible with the Constitution. Such a provision would make the corresponding information available only under the data transfer regulations in the laws governing the agency concerned. Those laws, in turn, could ensure specific thresholds for interference, which are required by constitutional law, and a sufficiently effective protection of legal interests. […] 228

E.

I.

The partial unconstitutionality of the challenged provisions does not result in their being declared void, but only in a finding that they are incompatible with the Basic Law. 229

Until a new provision is enacted, but no later than 31 December 2014, the provisions may continue to be applied, subject to the following stipulations: Except in an emergency under § 5 sec. 2 ATDG, the use of the counter-terrorism database is permissible only if access to the data of contact persons under § 2 sentence 1 no. 3 ATDG and to data resulting from interferences with the secrecy of telecommunications and the fundamental right to inviolability of the home is excluded, and if it is ensured that for searches of the extended basic data, a match only results in access to information under § 3 sec. 1 no. 3 ATDG, but not information under § 3 sec. 1 no. 1a ATDG. As soon as access to data of contact persons and data that derive from interferences with the secrecy of telecommunications and the fundamental right to inviolability of the home cannot be granted any more, these data also may no longer be used in emergencies under § 5 sec. 2 ATDG. 230

[…] 231-232

II.

The decision under C. is unanimous; otherwise there were partial dissents. […] 233

Kirchhof Gaier Eichberger

Schluckebier Masing Paulus

Baer Britz

Bundesverfassungsgericht, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07 - Rn. (1 - 233), http://www.bverfg.de/e/rs20130424_1bvr121507en.html

ECLI ECLI:DE:BVerfG:2013:rs20130424.1bvr121507