Headnotes

to the Judgment of the First Senate of 24 April 2013

1 BvR 1215/07

1. **The general structure of the counter-terrorism database, a joint database for various security authorities set up for the purpose of combating international terrorism whose function is essentially limited to facilitating inter-agency information requests and whose data may only be used for operational [police] measures in acute and exceptional cases of urgency, is compatible with the Constitution.**

2. **In light of the fundamental right to informational self-determination, statutory provisions that allow for data sharing between police authorities and intelligence services are subject to more stringent constitutional requirements. Fundamental rights give rise to the principle of separation of police and intelligence data that only permits such data sharing in exceptional cases.**

3. **Where a joint database for security authorities such as the counter-terrorism database is established, it requires a statutory framework that sufficiently specifies the data to be entered into it and its permissible uses in line with the prohibition of excessive measures. The Counter-Terrorism Database Act does not fully meet these requirements, notably with regard to the determination of the participating authorities, the large number of persons whose data is entered on grounds of potential ties with terrorism, the inclusion of data on 'contact persons', the [direct] use of extended data that is normally concealed from other authorities and the powers conferred upon security authorities to further specify which data is to be stored. The Act also falls short with regard to ensuring effective oversight.**

4. **The unrestricted inclusion in the counter-terrorism database of data obtained through interferences with the privacy of correspondence and telecommunications and the right to the inviolability of the home violates Article 10(1) and Article 13(1) of the Basic Law.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 1215/07 -

IN THE NAME OF THE PEOPLE

In the proceedings
on the constitutional complaint of

Mr S…,

– authorised representative: …

against the Act on Establishing a Standardised Central Counter-Terrorism Database for Police Authorities and Intelligence Services of the Federation and the *Länder* of 22 December 2006 (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:

JUDGMENT

1. **a) § 1(2) and § 2 first sentence no. 3 of the Counter-Terrorism Database Act of 22 December 2006 (BGBl I, p. 3409) are incompatible with Article 2(1) in conjunction with Article 1(1) of the Basic Law.**

   b) § 2 first sentence no. 1 lit. b of the Counter-Terrorism Database Act, regarding the element of 'supporting a group that supports a terrorist organisation', and § 2 first sentence no. 2 of the Counter-Terrorism Database Act, regarding the element of 'endorsing' [unlawful violence], are incompatible with Article 2(1) in conjunction with Article 1(1) of the Basic Law.

c) § 5(1) second sentence no. 1 lit. a of the Counter-Terrorism Database Act is incompatible with Article 2(1) in conjunction with Article 1(1) of the Basic Law insofar as it provides access to information pursuant to § 3(1) no. 1 lit. a of the Act when a search yields a match in the extended data.

d) § 3(1) first sentence no. 1 lit. b and § 10(1) of the Counter-Terrorism Database Act are incompatible with Article 2(1) in conjunction with Article 1(1) of the Basic Law to the extent that they lack certain supplementary provisions as set forth in the reasons.

e) For the rest, § 2 first sentence no. 2 and § 10(1) of the Counter-Terrorism Database Act must be interpreted in conformity with the Constitution as set forth in the reasons.

2. § 2 first sentence nos. 1 to 3, § 3(1) no. 1, § 5(1) and (2) as well as § 6(1) and (2) of the Counter-Terrorism Database Act are incompatible with Article 10(1) and Article 13(1) of the Basic Law to the extent that they apply to data that is stored in a concealed manner pursuant to § 4 of the Counter-Terrorism Database Act and was obtained through interferences with the privacy of telecommunications and the fundamental right to the inviolability of the home.

3. The provisions held to be incompatible with the Basic Law continue to apply until new provisions have been enacted, but no longer than 31 December 2014, subject to the following conditions: except in acute cases of urgency pursuant to § 5(2) of the Counter-Terrorism Database Act, the use of the counter-terrorism database is only permissible if it is guaranteed that there is no access to data of contact persons (§ 2 first sentence no. 3 of the Act) or to data obtained through interferences with the privacy of telecommunications and the fundamental right to the inviolability of the home, and that data access is limited to information pursuant to § 3(1) no. 3 of the Act in the event that searches of the extended data yield a match; where access to data of contact persons and data obtained through interferences with the privacy of telecommunications and the fundamental right to the inviolability of the home is ruled out, as set forth above, this data may no longer be used, not even under the urgency exceptions set out in § 5(2) of the Act.

4. […]

5. […]

REASONS:

A.

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

I.

The complainant challenges the Counter-Terrorism Database Act enacted by Art. 1 of the Act on Establishing Joint Databases for Police Authorities and Intelligence Services of the Federation and the *Länder* (Joint Databases Act) of 22 December 2006 (BGBl I, p. 3409). […] 2

1. The Counter-Terrorism Database Act provides the statutory basis for the counter-terrorism database, a joint database for police authorities and intelligence services of the Federation and the *Länder* that serves to combat international terrorism. This database facilitates and expedites information sharing between the respective police authorities and intelligence services by allowing all participating authorities to more quickly find and more easily access certain information held by the individual authorities in the context of the fight against international terrorism. 3

a) § 1 of the Counter-Terrorism Database Act provides that the counter-terrorism database is maintained as a joint and standardised central database by the Federal Criminal Police Office (*Bundeskriminalamt*). It also determines the participating authorities, which pursuant to § 1(1) of the Counter-Terrorism Database Act include: the Federal Criminal Police Office and, in conjunction with § 58(1) of the Federal Police Act and § 1(3) no. 1 of the Ordinance on the Competences of the Federal Police Authorities, the General Federal Police Headquarters (*Bundespolizeipräsidium*), as well as the criminal police offices of the *Länder* (*Landeskriminalämter*), the offices for the protection of the Constitution of the Federation and the *Länder* (*Verfassungsschutzbehörden*), the Military Counter-Intelligence Service (*Militärischer Abschirmdienst*), the Federal Intelligence Service (*Bundesnachrichtendienst*) and the Central Office of the German Customs Investigation Service (*Zollkriminalamt*). […] 4

b) § 2 of the Counter-Terrorism Database Act provides that authorities must store data already obtained [through other measures] in respect of certain persons or objects in the counter-terrorism database. Data must be stored in this manner if information obtained by the police or intelligence services indicates that the data relates to persons or objects that fall within the categories specified in § 2 first sentence nos. 1 to 4 of the Counter-Terrorism Database Act, and that knowledge of the data is necessary for investigating or combating international terrorism in connection to Germany. Pursuant to § 2 first sentence no. 1 of the Counter-Terrorism Database Act, the data to be stored in the database primarily concerns persons that either belong to or are closely associated with international terrorist organisations or groups. Pursuant to § 2 first sentence no. 2 of the Counter-Terrorism Database Act, data is furthermore 5

to be stored on individuals who unlawfully use, support, prepare, endorse or intentionally incite violence as a means to advance their political or religious interests internationally. § 2 first sentence no. 3 of the Counter-Terrorism Database Act also provides that data be stored on persons who were in contact with the persons laid down in no. 1 and no. 2 [referred to as 'contact persons'], provided that the contact was not merely brief and incidental and that the relevant data can be expected to yield information contributing to the investigation of or fight against international terrorism.

c) § 3(1) of the Counter-Terrorism Database Act determines which data is to be stored on the persons and objects specified in § 2 first sentence nos. 1 to 4 of the Counter-Terrorism Database Act. The provision distinguishes between basic data (*Grunddaten*) […] as provided for in § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act and extended data (*erweiterte Grunddaten*) as provided for in § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act. 6

Basic data must be stored on all persons falling under one of the groups listed in § 2 first sentence nos. 1 to 3 of the Counter-Terrorism Database Act. The provision defines various categories of general personal information as basic data, such as address data, special physical characteristics, languages and dialects spoken by that person, photographs and the respective grounds for storing the data pursuant to § 2 of the Counter-Terrorism Database Act. As regards extended data, § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act provides that such data only be stored in respect of the persons specified in § 2(1) nos. 1 and 2 of the Counter-Terrorism Database Act and in respect of contact persons if there are factual indications that they have knowledge of terrorism-related activities. § 3(1) no. 1 lit. b aa to rr of the Counter-Terrorism Database Act lists the categories of extended data. This data includes, *inter alia*, subscriber lines and telecommunication devices (aa), bank details (bb), ethnic origin (gg), religious affiliation (hh), skills relevant to terrorist activities (ii), information regarding education and training (jj), information regarding work in important infrastructure facilities (kk), information regarding propensity for violence (ll), and locations and areas visited that serve as meeting points for persons suspected of terrorism (nn). 7

[…] 8-9

To the extent that it is mandated by particular confidentiality interests or protected interests of affected persons, § 4 of the Counter-Terrorism Database Act allows for restricted or concealed storage of data. […] 10

d) § 5(1) of the Counter-Terrorism Database Act governs access to the stored data in standard cases. § 5(1) first sentence of the Counter-Terrorism Database Act allows participating authorities to submit requests in an automated procedure if the information is necessary for carrying out their tasks related to combating or investigating international terrorism. This power to access the database, which is not limited to searches for a particular name, enables these authorities to search all data sets, which includes both directly accessible data and data stored in a concealed manner 11

as well as both basic data and extended data; it also allows for searches of free text entries [containing additional non-standardised information such as comments or observations]. If a person-related search request yields a match, the requesting authority receives access to the basic data and the information which authority entered the data. Yet pursuant to § 5(1) third and fourth sentence of the Counter-Terrorism Database Act, the authority searching the database only receives access to the extended data in the event of a match if the authority that entered the data specifically grants access in the individual case upon special request in accordance with the applicable data transfer provisions. Regardless of the foregoing, where searches yield a match in the extended data, the corresponding basic data is transferred without any further conditions, independent of a possible accessing of the extended data itself.

Pursuant to § 6(1) first sentence of the Counter-Terrorism Database Act, the authority that submitted the request may only use the data it accessed [in the automated procedure] under § 5(1) of the Counter-Terrorism Database Act to verify whether the match can actually be attributed to the person sought, and to prepare and substantiate a request for an individual data transfer. 12

e) In urgent cases, § 5(2) first sentence of the Counter-Terrorism Database Act allows the authority that submitted the request to directly access the extended data that belongs to a positive match. […] 13

Where the requesting authority directly accessed extended data in an urgent case, this data may, pursuant to § 6(2) of the Counter-Terrorism Database Act, only be used to the extent that it is imperative to avert a present danger (*gegenwärtige Gefahr*) related to the fight against international terrorism. […] 14

§ 7 of the Counter-Terrorism Database Act provides that the transfer of information following a request pursuant to § 6(1) first sentence of the Counter-Terrorism Database Act is governed by the applicable transfer provisions. 15

f) § 8 of the Counter-Terrorism Database Act provides that both the authority that entered the data and the requesting authority have a shared responsibility for data protection. The requesting authority is responsible for ensuring that its request is permissible, while the authority that entered the data remains responsible for collecting the data in the first place, for ensuring that entering the data into the database was permissible and for ensuring that the data is correct and up-to-date. § 9 of the Counter-Terrorism Database Act provides for the documentation of any data access for the purposes of oversight in terms of data protection. Pursuant to § 10(1) of the Counter-Terrorism Database Act, responsibility for such oversight lies with the Data Protection Officer of the Federation and – subject to the respective *Land* laws – the data protection officers of the *Länder*. 16

§ 10(2) of the Counter-Terrorism Database Act sets out to what extent affected persons must be notified. The provision distinguishes between directly accessible and concealed data. […] 17

§ 11 of the Counter-Terrorism Database Act sets out the requirements for the correction, deletion and blocking of data, and § 12 of the Counter-Terrorism Database Act governs what details the Federal Criminal Police Office has to specify in its order to set up the database. […] 18

g) […] 19

2. […] 20-33

3. […] 34-37

4. […] 38-39

5. Various data protection officers performed audits at participating authorities with respect to the counter-terrorism database. The Federal Officer for Data Protection and Freedom of Information audited data processing at the Federal Criminal Police Office, at the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), and at the Federal Intelligence Service (*Bundesnachrichtendienst*). […] Further audits were performed by the *Land* data protection officers. 40

II.

[…] 41-51

III.

Statements on the constitutional complaint were submitted by the Federal Government, the Federal Officer for Data Protection and Freedom of Information, the Schleswig-Holstein Independent *Land* Centre for Data Protection (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*), the Berlin Officer for Data Protection and Freedom of Information, and the Baden-Württemberg Officer for Data Protection. 52

[…] 53-77

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(1) in conjunction with Art. 1(1) of the Basic Law, of the privacy of correspondence and telecommunications under Art. 10(1) of the Basic Law, of the inviolability of the home under Art. 13(1) of the Basic Law and, in conjunction with 80

these fundamental rights, a violation of the guarantee of legal protection under Art. 19(4) of the Basic Law.

[…] 81

II.

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

1. [For the constitutional complaint to be admissible,] the complainant must be directly affected. This is the case here. A complainant is only directly affected by a statutory provision if the provision as such interferes with the complainant's rights without requiring any further implementation measures. If execution of a statutory provision requires – either by law or based on the practice of authorities – a specific implementation measure that is contingent upon a deliberate decision by the executing authority, complainants must generally challenge this implementation measure and exhaust all available legal remedies before lodging a constitutional complaint (BVerfGE 1, 97 <101 *et seq*.>; 109, 279 <306>; established case-law). However, it must be presumed that complainants are directly affected if seeking legal recourse is not possible because they have no way of knowing whether the respective implementation measure was carried out. In such cases, complainants can lodge a constitutional complaint directly against a statute, just as in cases where fundamental rights are affected by a statute without any intermediary implementation measure (cf. BVerfGE 30, 1 <16 and 17>; 113, 348 <362 and 363>; 120, 378 <394>; established case-law). The case at hand fits these conditions. Under the challenged provisions, it is in principle not possible for the complainant to obtain reliable knowledge of the storage or use of his data. 83

Even though the complainant can request information on the storage of his data pursuant to § 10(2) of the Counter-Terrorism Database Act, and bring an *ex post* challenge before the courts, this does not lead to a different result. On that basis, the complainant could only challenge storage of his data that actually occurred at a certain time; however, he would not be able to challenge the fact that such data storage can occur at any time beyond his control and without him knowing about it – which is what he actually seeks to challenge with his constitutional complaint. […] 84

2. […] 85-87

C.

There is no need for requesting a preliminary ruling from the Court of Justice of the European Union pursuant to Art. 267 TFEU to clarify the scope of fundamental rights protection under EU law in respect of data sharing among various security authorities through a joint database as provided for by the Counter-Terrorism Database Act. This also holds true with regard to the fundamental right to the protection of personal data 88

under Art. 8 of the Charter of Fundamental Rights of the European Union. The EU fundamental rights laid down in the Charter are not applicable in the case at hand. The challenged provisions must be measured against the fundamental rights laid down in the Basic Law given that the provisions are not determined by EU law (cf. BVerfGE 118, 79 <95>; 121, 1 <15>; 125, 260 <306 and 307>; 129, 78 <90 and 91>). Thus, the present proceedings do not concern the implementation of EU law by the Member States, in which case they would be bound by the Charter of Fundamental Rights (Art. 51(1) first sentence of the Charter).

[…] 89-91

D.

The constitutional complaint is in part well-founded. 92

I.

The challenged provisions interfere with the right to informational self-determination (Art. 2(1) in conjunction with Art. 1(1) of the Basic Law), the right to the privacy of correspondence and telecommunications (Art. 10(1) of the Basic Law) and the right to the inviolability of the home (Art. 13(1) of the Basic Law). 93

1. §§ 1 to 6 of the Counter-Terrorism Database Act govern the storage and use of personal data, and therefore affect the scope of protection of the right to informational self-determination. To the extent that the data stored and used was collected through interferences with Art. 10(1) or Art. 13(1) of the Basic Law, any subsequent use must also be measured against these fundamental rights (cf. BVerfGE 125, 260 <313>; established case-law). 94

2. The challenged provisions interfere with these fundamental rights. First of all, the linking of data from different sources resulting from the obligation to store data imposed in §§ 1 to 4 of the Counter-Terrorism Database Act amounts to an interference. The fact that the data had already been collected by the authorities in other contexts does not lead to a different result; the data is combined and processed based on distinct criteria in order to make it available to authorities other than those that collected the data for their purposes. Further interferences result from §§ 5 and 6 of the Counter-Terrorism Database Act, which govern the use of this data for the purpose of searches in the database; from the possibility to access the basic data in the event of a match pursuant to § 5(1) first and second sentence and § 6(1) first sentence of the Counter-Terrorism Database Act; as well as from the possibility to [directly] access the extended data in urgent cases pursuant to § 5(2) and § 6(2) of the Counter-Terrorism Database Act. 95

II.

Formally, the challenged provisions are compatible with the Constitution. In particular, the Federation has legislative competence. 96

[…] 97-104

III.

The general structure of the counter-terrorism database established by the challenged provisions is compatible with the right to informational self-determination under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law. The principle of proportionality does not *per se* rule out such a database, which, in the context of investigating and combating international terrorism, aims to facilitate requests for information, and, in urgent cases, directly serves to avert dangers to public security. However, the specific statutory design, too, must satisfy the requirements of proportionality. 105

1. The counter-terrorism database has a legitimate aim. It primarily serves to inform security authorities, in a quick and easy manner, whether other security authorities have relevant information about specific persons associated with international terrorism. It thus aims to provide preliminary information, which allows the authorities to request further information from other authorities more quickly and efficiently, and which, in urgent cases, also allows for a preliminary assessment of dangers as the basis for further action. The legislative aim is neither to facilitate the general sharing of personal data among all security authorities nor to eliminate all informational barriers between these authorities; this would undermine the principle of purpose limitation, and therefore be impermissible from the outset. Rather, the legislative intent behind creating the database is to allow for somewhat easier information sharing within a limited context. This facilitated information sharing does not affect the applicability of the provisions on individual data transfers set out in other areas of ordinary legislation, which remain subject to statutory limitations, and it is limited to the fight against international terrorism. While the term ‘terrorism’ as such can have different meanings, the Counter-Terrorism Database Act refers to § 129a of the Criminal Code, as follows from § 2 first sentence no. 1 lit. a of the Counter-Terrorism Database Act, which is the central provision determining the persons whose data is included in the database. Accordingly, in the Counter-Terrorism Database Act, the term ‘terrorism’ refers to specifically defined serious offences that criminalise acts seeking to intimidate the public or targeting the fundamental structures of a state or an international organisation. This understanding of the term does not raise any constitutional objections. 106

2. The challenged provisions are also suitable and necessary for achieving this purpose. The data storage obligations imposed in §§ 1 to 4 of the Counter-Terrorism Database Act create a basic data inventory that is made available to the participating authorities pursuant to § 5(1) and § 6(1) first sentence of the Counter-Terrorism Database Act. It serves to allow those authorities to prepare further requests for information, and to provide them with information needed to avert specific dangers (*konkrete Gefahren*) in particularly urgent cases pursuant to § 5(2) and § 6(2) of the Counter-Terrorism Database Act. Other instruments that would be less intrusive but equally 107

effective in achieving these aims are not ascertainable.

3. The general structure of the Counter-Terrorism Database Act is also compatible with the principle of proportionality in its strict sense. 108

The principle of proportionality in its strict sense requires that in an overall assessment, the severity of legislative fundamental rights restrictions not be disproportionate to the weight of the reasons invoked to justify such restrictions. In this respect, an appropriate balance must be struck between the weight of the interference resulting from the statutory provisions and the legislative aim pursued, and between the conflicting interests of the individual and the general public (cf. BVerfGE 100, 313 <375 and 376>; 113, 348 <382>; 120, 378 <428>; established case-law). 109

The challenged provisions give rise to interferences of considerable weight (see a below). Yet they also serve weighty public interests (see b below). Based on a balancing of these conflicting interests, the establishment and general nature of the counter-terrorism database are not *per se* objectionable under constitutional law; however, the design of the framework specifying the details of the database must contain clear and sufficiently restrictive provisions, including for ensuring effective oversight of its application in practice (see c below). 110

a) The possibilities of information sharing created by the challenged provisions are of considerable weight. […] It increases the severity of the interference that the database allows for information sharing among a large number of security authorities with very different mandates, including information sharing between intelligence services and police authorities (see aa below). Yet it mitigates the severity of the interference that information sharing is limited to already collected data, that the database is designed as a joint database focusing on facilitating requests for information, and that its sole aim is to investigate and combat international terrorism (see bb below). 111

aa) It increases the severity of the interference resulting from the counter-terrorism database that it allows for information sharing among a large number of security authorities, including authorities with very different tasks and powers. It is particularly significant here that the database also extends to information sharing between intelligence services and police authorities. 112

(1) Where personal data is concerned, the powers to collect and process data conferred on the different security authorities are tailored to, and limited by, the respective authority's specific tasks. Under constitutional law, the use of personal data is thus subject to purpose limitations, it cannot readily be shared with other authorities. Security authorities have different remits, depending on their respective domain and role in the federal order; regarding data protection, this division of tasks also has a special fundamental rights dimension. It is not therefore a flaw in the organisational structure of the state that information cannot be shared comprehensively and freely among the various security authorities; rather, this structure is in principle intended and required by the Constitution, as it derives from the principle of purpose limitation 113

in respect of data protection.

However, the constitutional principle of purpose limitation in respect of data does not prevent the legislator from changing the original purpose [for which data was collected] if such a change in purpose is justified by public interests that outweigh the protected fundamental rights interests (cf. BVerfGE 100, 313 <360>; 109, 279 <375 and 376>; 110, 33 <69>). When assessing whether information sharing between different authorities is proportionate, it is particularly significant whether the different informational contexts are comparable. The more the authorities' tasks, powers and modes of operation differ, the greater the weight accorded to data sharing [in the proportionality assessment]. Therefore, for changes in purpose to be proportionate, it is particularly relevant to what extent the requirements regarding data collection by the transferring authority, or in the present case, the authority entering data into the database, correspond to the requirements under which the requesting authority may collect data. Accordingly, a change in purpose is not permissible if it circumvents fundamental rights-related restrictions regarding the use of certain investigation methods; this is the case where, even on the basis of statutory powers, the information could not have been lawfully obtained for the changed purpose, neither with the investigatory means applied nor by other means (cf. BVerfGE 109, 279 <377>; 120, 351 <369>). Accordingly, the Federal Constitutional Court repeatedly held that the further use [for other purposes] of data obtained through interferences with the privacy of telecommunications is only constitutional if the changed purposes could also have justified the original data collection (cf. BVerfGE 100, 313 <360, 389>; 109, 279 <375>; 110, 33 <73>). The Court found it necessary that procedural safeguards, such as labelling and documentation requirements, be put in place in order to guarantee that these requirements are met (cf. BVerfGE 65, 1 <46>; 113, 29 <58>; 124, 43 <70>). The same also applies to changes in purpose of data processing measures if data was obtained through interferences with the right to informational self-determination. Constitutional requirements for collecting, storing and processing data must not be circumvented by allowing authorities which, within their remit, are subject to less stringent requirements to transfer data to authorities that are subject to more stringent requirements. 114

(2) Thus, the combination of data held by intelligence services with data held by police authorities is of increased weight and is generally subject to strict constitutional limits, because the tasks of police authorities and intelligence services differ considerably. Therefore, they are subject to fundamentally different requirements with respect to the openness with which they perform their tasks and with respect to data collection. 115

(aa) Intelligence services are tasked with precautionary investigations of threat situations before actual dangers even arise. […] 116

Given that the mandate of intelligence services largely concerns precautionary measures carried out before actual dangers arise, they have far-reaching powers in re- 117

spect of data collection; these powers are neither limited to specifically defined areas of activity, nor subject to detailed rules regarding the means that may be employed. […] Without prejudice to various constitutional requirements that apply in this respect but are not at issue in the present proceedings, these powers reflect the broad mandate conferred upon the intelligence services, and are characterised by relatively low thresholds for carrying out measures constituting interferences. Furthermore, intelligence services generally collect data covertly. They are not subject to the principle of the overtness of data collection and are largely exempt from transparency and notification requirements vis-à-vis affected persons. Accordingly, indiviudals have few possibilities of legal protection. In part, legal recourse is even entirely replaced by political oversight (cf. Art. 10(2) second sentence of the Basic Law).

At the same time, the permissible investigative aims of measures carried out by intelligence services are restricted in order to compensate for the broad data collection powers. Even though the exact powers of different intelligence services differ, their investigatory mandate is essentially limited to observing and reporting on fundamental threats that might destabilise the community as a whole, in order to allow for an assessment of the security situation at the political level. The overall aim pursued is not to carry out operational measures to avert dangers to public security, but to gather political intelligence. […] 118

This mandate of the intelligence services, which is limited to precautionary measures for gathering political intelligence, is also reflected in a restriction of the services' powers in other respects: they do not have police powers, nor may they request that the police carry out measures for which the intelligence services themselves have no authorisation through inter-agency administrative assistance (*Amtshilfe*). […] 119

(bb) These tasks and powers differ fundamentally from those of police and security authorities. It is for these authorities to prevent, avert and prosecute criminal acts, and to avert other dangers to public security and order. Their mandate is informed by operative action and in particular includes the power to execute measures against individuals, if necessary by force. At the same time, their tasks are defined in statutory law in a more detailed and restrictive manner and the powers conferred upon them to perform these tasks are subject to a diverse range of substantive and procedural requirements. It is true that some of the tasks assigned to police authorities do fall within the category of purely precautionary action taken before a danger arises. However, their powers to take action against individuals may in principle only be exercised based on specific grounds; they generally require indications of a suspicion of criminal conduct or the existence of a danger. The powers to collect and process data conferred upon the police authorities reflect this mandate. Given that such powers can ultimately be used to prepare and justify coercive measures [against individuals], including interferences with personal liberty, they are more narrowly and precisely defined by law than the powers of intelligence services, and the law distinguishes between different powers in various ways. Where these powers relate to data handling, they also generally require specific grounds, albeit to differing degrees, such as the 120

existence of a danger or the suspicion of a crime. To the extent that the legislator permits, in exceptional cases, data retention not based on specific grounds as a precaution or merely for the purpose of preventing dangers or criminal acts, this requires special justification, and is subject to more stringent constitutional requirements (cf. BVerfGE 125, 260 <318 *et seq*., 325 *et seq*.>).

Accordingly, the police generally act overtly, and their handling of data is largely subject to the principle of overtness and transparency. […] 121

Thus, the legal order distinguishes between the police, which generally work overtly, are tasked with operational measures and are subject to detailed statutory regimes, and the intelligence services, which generally work covertly, with powers limited to observation and investigation as precautionary action before a danger actually arises, to provide political intelligence and advice and therefore allowed to act within a less detailed statutory framework. The legal order does not allow for a secret police. 122

(cc) In light of these differences, provisions that allow for data sharing between the police and intelligence services are subject to more stringent constitutional requirements. In this regard, the fundamental right to informational self-determination gives rise to the principle of separation of police and intelligence data (*informationelles Trennungsprinzip*), according to which data may in principle not be shared between the intelligence services and police authorities. Deviations from this principle are only permissible in exceptional cases. If such exceptions are made in relation to operational measures [of the police], they give rise to particularly serious interferences. Data sharing between intelligence services and police authorities that might lead to operational police action being taken must therefore, in principle, serve an exceptionally significant public interest which can justify the accessing of information under the easier conditions normally reserved for the intelligence services. This must be ensured by sufficiently specific and qualified thresholds for carrying out data sharing constituting such an interference, which must be set out in clear statutory provisions; moreover, the data sharing carried out on this basis must not circumvent the thresholds for interferences applicable to obtaining the relevant data in the first place. 123

bb) However, it reduces the severity of the interference resulting from the counter-terrorism database that it is designed as a joint database, which is essentially limited to facilitating requests for information, and which only permits use of the data for operational police action in exceptional emergencies. 124

(1) The challenged provisions set out the counter-terrorism database as an instrument that – except in urgent cases pursuant to § 5(2) and § 6(2) of the Counter-Terrorism Database Act – does not provide information which the respective authorities can use directly in the exercise of their tasks, especially not for operational police purposes; rather, it provides information only as a basis for [requesting] further data transfers. […] Therefore, with regard to the basic data pursuant to § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act, the counter-terrorism database does not autho- 125

rise the sharing of information for direct use [by the requesting authority] in the exercise of its tasks, but only prepares the basis for such information sharing. This applies all the more to the extended data pursuant to § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act, which the authorities may generally only access subject to the transfer provisions under the respective statutory regimes applicable in the specific case (§ 5(1) fourth sentence of the Counter-Terrorism Database Act).

Thus, the Counter-Terrorism Database Act mainly refers to the specific statutory bases for data transfers set out in applicable legislation, upholding the rule-of-law limits deriving therefrom. Ultimately, it ensures that – apart from cases set out in § 5(2) and § 6(2) of the Counter-Terrorism Database Act – data sharing for direct use in investigating and combating international terrorism is permissible only subject to the statutory requirements of the transfer provisions applicable in the specific case. […] 126

(2) The purpose of the counter-terrorism database, which is essentially limited to facilitating requests for information, lessens the weight of interference significantly; yet even in light of this purpose, the weight of interference remains considerable. […] 127

For affected persons, being registered in such a database can be a considerable burden. Once a person has been included in the database, they must expect to be classified as persons associated with terrorism based on [matches] from search requests and – based on further requests for data transfers facilitated by the database – to be subjected to intrusive measures as a result thereof. The consequences of such a classification can be considerable and might put individuals in a difficult situation; at the same time, the persons concerned are not even aware of this classification, nor do they have any feasible options to defend themselves against it. It increases the severity of the interference that the data is entered into the database without background information on its specific context, and may in part be based on mere prognoses and subjective assessments by the respective authority, which are by definition uncertain at best. Ultimately, individuals may face considerable impairments despite not having prompted the measures themselves. Intrusive measures cannot, in principle, directly result from the use of the data from the counter-terrorism database based on the challenged provisions alone, but can only be expected as an indirect effect of these provisions in conjunction with other legislation; however, this does not change the fact that the counter-terrorism database increases the likelihood of such measures. 128

(3) The counter-terrorism database gives rise to interferences of particular weight where it also allows for information sharing between intelligence services and police authorities in urgent cases; in this context, the information may be used directly by the receiving authority to avert a specific danger to public security, i.e. for operational purposes. 129

b) In principle, the establishment of the counter-terrorism database is compatible with the prohibition of excessive measures (*Übermaßverbot*). The weight of interference for affected individuals must be balanced against the public interest in targeted 130

information sharing between the different security authorities for the purpose of investigating and combating international terrorism and allowing more accurate assessments to avert dangers to public security in important and urgent cases.

131 The legislator may attach considerable significance to the establishment of a central joint database for targeted information sharing for the purpose of investigating and combating international terrorism. Given the large number of authorities responsible for these tasks, it is particularly important to ensure that information sharing among them is effective. […]

132 […]

133 When assessing the significance of such a database, it must be taken into account that the effective fight against terrorism carries great weight for a democratic and free society. Criminal acts that qualify as terrorism, against which the Counter-Terrorism Database Act is directed (see D III 1 above), aim to destabilise society and, to this end, comprise attacks on the life and limb of random third parties, in a ruthless instrumentalisation of others. They are directed against the pillars of the constitutional order and society as a whole. Our constitutional order requires that such attacks not be considered acts of war or a state of emergency, which would lead to a suspension of certain requirements deriving from the rule of law, but that they be qualified as criminal acts that must be countered with the means available to the state under the rule of law. At the same time, the proportionality assessment required under the principle of the rule of law must accord considerable weight to the fight against terrorism (cf. BVerfGE 115, 320 <357 and 358>).

134 c) Given these conflicting interests, an overall assessment does not raise constitutional objections against the general structure of the counter-terrorism database as an instrument for facilitating information requests and as a source of information for assessing dangers in acute cases of urgency. However, the statutory framework governing the database only satisfies the principle of proportionality in its strict sense if the provisions are clear and, in their substantive details, sufficiently limited regarding what data must be stored in the database and the way in which this data may be used, and if qualified oversight requirements are provided for and observed (BVerfGE 125, 260 <325>).

135 aa) The general structure set out by the legislator, which establishes the counter-terrorism database as a joint database to facilitate requests for information, is not objectionable under constitutional law. It is not disproportionate in and of itself to include in the database basic identifying data in respect of specific persons that are likely associated with international terrorism, nor to make this data available to the participating authorities for the purpose of facilitating requests for information. The fight against terrorism justifies the combination of intelligence data and police data in the present case given that the shared data is only used to prepare individual data transfers that are subject to statutory limitations. […]

However, the database must be designed in such a way that information sharing is governed by clear provisions and sufficiently limited. This also applies with regard to determining the participating authorities, the persons whose data is stored in the database and the scope of data to be stored on them, and with regard to further specifying the statutory regime governing use of this data. Moreover, effective oversight must be ensured (see D IV below). 136

bb) Due to the great importance of preventing terrorist attacks, it is also not objectionable that the legislator intends to provide a source of information in the form of the counter-terrorism database that also allows the participating authorities to conduct a preliminary assessment of dangers as a starting point for further action in acute cases of urgency. […] 137

IV.

Based on these standards, the challenged provisions fail to satisfy, in various respects, the requirements regarding a sufficiently specific statutory design of the counter-terrorism database that adheres to the prohibition of excessive measures. To this extent, they violate the right to informational self-determination. 138

1. § 1(2) of the Counter-Terrorism Database Act, which provides for the possible participation of other police authorities in the counter-terrorism database, is incompatible with the requirement of specificity. 139

a) The requirement of specificity serves to ensure that the law subjects the government and administration to standards that direct and limit their actions, and that the courts can effectively review the lawfulness of their actions. Furthermore, clear and specific legal provisions ensure that affected persons can take precautions against potentially intrusive measures (cf. BVerfGE 110, 33 <52 *et seq*.>; 113, 348 <375 *et seq*.>; 120, 378 <407 and 408>). […] The specificity requirements that must be met depend on the severity of the interferences with fundamental rights effected by a provision or measures taken pursuant to that provision. 140

According to these standards, the authorities participating in the counter-terrorism database must be determined either directly by law, or by an ordinance based on a law. The determination which authorities must enter their data into the database, and which authorities may access this data, is decisive for the scope and content of the database as well as for the extent of further use of the data. This is an essential element of the legislative framework that requires a clear, specific and legally binding determination. […] 141

b) § 1(2) of the Counter-Terrorism Database Act does not satisfy, neither by itself nor in conjunction with § 12 of the Counter-Terrorism Database Act as the provision mandating the establishment of the database, the special requirements relating to the determination in statutory law which other police authorities can participate in the counter-terrorism database. 142

aa) § 1(2) of the Counter-Terrorism Database Act does not provide a sufficiently clear statutory determination from which the participating authorities can be directly derived. […] If the participating authorities could be derived directly from the law with sufficient specificity, it would not necessarily be problematic that the individual authorities are not listed expressly (cf. BVerfGE 130, 151 <199, 203>). Yet this is not the case here. § 1(2) of the Counter-Terrorism Database Act describes the participating authorities only in broad, general terms that are subject to interpretation. […] 143

bb) Nor can a sufficiently clear determination of the participating authorities be derived from § 1(2) of the Counter-Terrorism Database Act in conjunction with § 12 no. 2 of the Counter-Terrorism Database Act, as the provision mandating the establishment of the database. It is not, in principle, objectionable to delegate the final determination of these authorities to the executive branch. […] However, if the legislator chooses to place the decision about the participating authorities in the hands of the executive, Art. 80(1) of the Basic Law requires that this be done in the form of an ordinance. 144

2. The provisions determining the group of persons whose data is included in the database are not compatible with the constitutional requirements in every respect. Some of these provisions violate the principle of specificity and the prohibition of excessive measures. Others require a restrictive interpretation in conformity with the Constitution. 145

a) There are no constitutional objections regarding § 2 first sentence no. 1 lit. a of the Counter-Terrorism Database Act. This provision requires the entering of data on persons suspected of belonging to or supporting a terrorist organisation, i.e. those who are the focus of effective counter-terrorism measures. This provision refers to statutory offences that already criminalise certain conduct long before it results in actual violations of legal interests, and it only requires “factual indications” for the conduct in question – even where it only concerns supporting acts. The provision thus grants authorities substantial discretion with regard to their subjective assessments, which entails many uncertainties [as regards the application in practice]. However, this is acceptable in relation to the counter-terrorism database, which – apart from acute and exceptional cases of urgency – only serves to facilitate requests for information, and, in that context, to enable participating authorities to refute or corroborate unconfirmed assumptions regarding suspicions of criminal conduct and dangers before formal investigations are even launched. When properly interpreted, the statutory prerequisites are still sufficient to ensure that data is not stored on the basis of mere speculation. […] 146

b) § 2 first sentence no. 1 lit. b of the Counter-Terrorism Database Act, which extends the scope of the data stored in the database to data of persons supporting terrorist organisations, is in part incompatible with the prohibition of excessive measures and thus unconstitutional. 147

aa) The provision is not objectionable to the extent that it includes persons who be- 148

long to a group that supports a terrorist organisation. […]

bb) However, the provision expands the scope of the database further in that it also includes persons who merely support such a supporting organisation. It is not ascertainable that the provision requires any link connecting the persons in question to terrorism. According to its wording, and the legislative purpose that plausibly derives from it, the provision thus also extends the obligation to store certain data in the database to data on persons who, long before a terrorist act is committed, support what they possibly believe to be an unsuspicious organisation, without being aware of any link to terrorism; an example would be persons supporting a nursery run by a mosque association which the authorities suspect of supporting terrorist organisations. Such an expansive approach, broadening the scope of application to include even persons with only remote links to the environment in which a terrorist organisation operates, violates the principle of legal clarity and is incompatible with the prohibition of excessive measures. […] 149

c) § 2 first sentence no. 2 of the Counter-Terrorism Database Act is not fully compatible with the Constitution. This provision, which targets individuals who might be associated with terrorism, combines a number of ambiguous and potentially broad legal terms. Following a tie in the Justices' vote, the terms 'unlawful violence' and 'intentional incitement to unlawful violence' cannot be declared unconstitutional. In the opinion of the four Justices who voted against a declaration of unconstitutionality in this respect – and whose view ultimately carries the decision pursuant to § 15(4) third sentence of the Federal Constitutional Court Act – the use of these legal concepts is compatible with the Basic Law as long as they are not interpreted in an overly broad manner (see aa below). In the opinion of the other four Justices, whose position ultimately does not prevail (§ 15(4) third sentence of the Federal Constitutional Court Act), the provision would have to be declared unconstitutional in this regard (see bb below). In the unanimous view of the Court, the mere 'endorsement' of unlawful violence within the meaning of this provision does in any case not provide sufficient grounds justifying the registration of personal data in the counter-terrorism database. To that extent, the provision violates the prohibition of excessive measures and is unconstitutional (see cc below). 150

aa) (1) The provision mainly hinges on the term 'unlawful violence'. This term has a very broad meaning in other parts of the legal order. It is true that based on a broad understanding, the concept of unlawful violence would not be a sufficient basis for classifying persons as being associated with terrorism given that it would not adequately limit the group of affected persons in accordance with the principle of proportionality, and therefore not provide sufficient grounds justifying the data storage under constitutional law. […] However, in light of the counter-terrorism database's aim to fight terrorist crime, this term must be interpreted to the effect that it only refers to violence immediately directed against life and limb, or characterised by the use of means that endanger the public. When interpreted in this way, the term 'unlawful' in § 2 first sentence no. 2 of the Counter-Terrorism Database Act is not objectionable 151

under the principle of proportionality with regard to determining the group of persons whose data is to be entered in the database.

(2) Furthermore, § 2 first sentence no. 2 of the Counter-Terrorism Database Act provides for the registration of both persons who use, support and prepare violence, and those who merely endorse or intentionally incite it with their actions. This would open up disproportionately broad possibilities for interference if mere general criminal intent (*Eventualvorsatz*), within the meaning attached to it in criminal law terminology, were deemed sufficient to establish an intentional incitement to violence. However, if, in this context, the element of intentional incitement to violence is attributed a meaning which only covers acts that deliberately aim to incite violence, this interpretation satisfies the principle of proportionality. 152

[*Translator's note*: The following sections are highlighted in italics in the German original to denote the opposing view of the four Justices who were in favour of declaring the provision unconstitutional:]

bb) In the opinion of the other four members of the Senate, which ultimately does not prevail pursuant to § 15(4) third sentence of the Federal Constitutional Court Act, § 2 first sentence no. 2 of the Counter-Terrorism Database Act must be declared unconstitutional in its entirety because of its lack of specificity and its overly broad scope. In their view, a narrow interpretation of the terms 'unlawful violence' and 'intentional incitement' that deviates from the established definitions of these terms in criminal law cannot lead to a different result. The attempt to interpret the provision in conformity with the Constitution is inconsistent and undermines the requirements of specificity in respect of data protection law. 153

(1) Significant elements of this provision are ambiguous, and are interpreted broadly elsewhere in the legal order – specifically, in criminal law, which is fundamental to the general understanding of legal terms –, to an extent that, in the context of the counter-terrorism database, is incompatible with the requirements of proportionality and the prohibition of excessive measures; the four members of the Senate whose position prevails concur with this finding […] 154

(2) [Yet in the opinion of the other four members of the Court whose position does not prevail,] the provision cannot be interpreted restrictively and thus brought in conformity with the Constitution. 155

(a) Such an interpretation is already ruled out for § 2 first sentence no. 2 of the Counter-Terrorism Database Act because the central term 'unlawful violence' in that provision was deliberately chosen by the legislator in order to keep the wording broad and open. The vagueness and overly broad scope of this term were explicitly criticised in the legislative process (BTPlenarprotokoll 16/71, p. 7100; Bundestag Committee on Internal Affairs, minutes no. 16/24, p. 55; A-Drucks 16(4)131 D, p. 10; A-Drucks 16(4)131 J, p. 10). Notably, a specific counter-proposal was submitted, putting forward a more restrictive definition based on § 129a(2) of the Criminal Code, 156

according to which unlawful violence was only recognised as grounds for storing data "if such violence was intended to seriously intimidate the population, to unlawfully coerce a state authority or an international organisation, or to destroy or significantly impair the fundamental political, constitutional, economic or social structures of a state or an international organisation, and if the person's actions threatened to inflict serious damage on a state or an international organisation" (cf. BTDrucks 16/3642, pp. 14 and 15). This was an attempt to narrow down the term in line with international and European frameworks on 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 legislator, however, made a deliberate decision to disregard this proposal – apparently in order to grant security authorities more latitude. Such a decision cannot be remedied through an interpretation in conformity with the Constitution.

(b) In addition, the provision cannot be interpreted in conformity with the Constitution for reasons deriving from fundamental principles of constitutional law. If the statutory basis for measures that constitute interferences has an open wording, as is the case here, and if, based on recognised definitions, its wording plausibly supports such a far-reaching interpretation, it cannot serve as a basis for the data processing measures at issue here as it fails to satisfy the principles of legal clarity and proportionality in that regard. The principle of legal clarity specifically serves to compel the legislator to make sufficiently clear decisions regarding the statutory prerequisites for interferences with fundamental rights, so as to sufficiently ensure that the prohibition of excessive measures is upheld. If the legislator fails to satisfy these constitutional requirements, the Federal Constitutional Court cannot remedy this failure through an interpretation in conformity with the Constitution. […] 157

[…] According to the Federal Constitutional Court's established case-law, the requirements of legal clarity and specificity in respect of data protection law are particularly stringent (cf. BVerfGE 65, 1 <46>; 118, 168 <187>; 120, 378 <408>) – and this especially holds true for the counter-terrorism database, given that it governs data sharing among security authorities prior to any formal investigation. As a result, data processing under the Counter-Terrorism Database Act differs, at the level of implementation, from other laws that are implemented by means of ordinary administrative acts: where laws are implemented by means of ordinary administrative acts, the implementing measure is directly addressed to the person concerned, includes a statement of reasons, and allows for judicial review in the individual case; by contrast, under the Counter-Terrorism Database Act, affected persons have no direct knowledge of the data processing measures concerning them. Such data processing measures remain informal, no reasons are provided to the affected individual, and there is generally no possibility of judicial review. […] 158

The qualified specificity requirements that derive from fundamental rights in respect of data protection are not rooted in excessive mistrust vis-à-vis the security authori- 159

ties. Rather, these requirements are in place to ensure that the prerequisites for data processing carried out by security authorities are set out in unequivocal terms, especially with regard to [early] stages during which the authorities' activities often involve a significant amount of data processing yet are subject to no or only few formal requirements; it is precisely in these stages that such an unequivocal framework provides the authorities with the clearest possible guidance in performing their demanding tasks, and also eases their burden in cases of doubt.

(c) It is also not necessary to undertake an interpretation in conformity with the Constitution out of respect for the legislator. It is true that with the Counter-Terrorism Database Act, the legislator designed a complex and nuanced concept; in various respects, the legislator showed restraint as required under the rule of law and genuinely endeavoured to ensure adequate data protection. However, constitutional review of the specific provisions implementing this concept cannot be based on an overall assessment of the political effort undertaken by the legislator. Rather, the Court must give effect to constitutional standards in all respects regardless of such considerations, and thereby ensure that the notion of the rule of law informing the general framework is not eroded through overly broad individual provisions incorporated therein. In this regard, *respect for the legislator actually requires that the Court refrain from designing a more restrictive data protection arrangement for the challenged provisions, and that it simply declare the provisions unconstitutional instead: Rather than interpreting the provisions [in conformity with the Constitution], and thus imposing an arrangement on the legislator that may seem sensible in light of the legislative aim, but that the legislator clearly did not wish to adopt – at least for the time being –, a declaration of unconstitutionality would again defer to the legislator the responsibility to define, in accordance with its competences, the appropriate limits. Technical or legislative reasons that would have made it particularly difficult for the legislator to accomplish this are not ascertainable.* 160

cc) The element 'endorsement of violence' is especially far-reaching. With this element, the legislator only refers to an attitude without requiring that this attitude must have resulted in activities promoting violence. The use of this element [in § 2 first sentence no. 2 of the Counter-Terrorism Database Act] is incompatible with the Constitution, and the provision is unconstitutional in this respect. This element must generally be considered excessive in scope, which can also not be remedied through an interpretation in conformity with the Constitution. The only example given in the explanatory memorandum to the law is that of hate preachers who publicly incite hatred and violence, an example which in principle does not raise constitutional concerns. However, from the wording of the provision, which generally appears to be further-reaching, it cannot be derived that its scope is limited to such cases. Rather, the wording suggests that the only decisive factor is whether a person's attitude amounts to endorsing violence. According to the wording, it is sufficient that the authorities infer such an attitude from factual indications. The use of such a criterion [in the legislative design], which is directly tied to the *forum internum* and therefore intrudes into 161

an individual's inalienable inner domain, is especially capable of having a chilling effect on the exercise of other fundamental freedoms, in particular freedom of faith and freedom of expression. The challenged provision uses subjective beliefs as such as its decisive element and thus relies on criteria that individuals cannot fully control and that cannot be influenced by law-abiding conduct. The registration of persons in the counter-terrorism database on the basis of such a criterion is incompatible with the prohibition of excessive measures. § 2 first sentence no. 2 of the Counter-Terrorism Database Act is unconstitutional in that respect.

d) § 2 first sentence no. 3 of the Counter-Terrorism Database Act is also unconstitutional. It provides for the inclusion of data on contact persons, which is incompatible with both the principle of specificity and the prohibition of excessive measures. 162

§ 2 first sentence no. 3 of the Counter-Terrorism Database Act provides that even mere contact persons of the persons specified in the preceding numbers of the provision must be included in the counter-terrorism database. […] 163

The recognition of contact persons as an additional group of persons on whom data can be entered in and shared through the database, including in the form of non-anonymised information, does not satisfy the requirements of specificity. It is impossible to predict on this basis which persons are in fact to be included in the database. […] 164

In view of the large, almost indeterminable number of persons potentially falling into the category of contact persons, the provision also violates the prohibition of excessive measures. Constitutional law does not generally rule out that data of contact persons, too, is made available in the counter-terrorism database. However, based on the purposes of the database, persons who do not already fall within the categories set out in numbers 1 and 2 of the provision, i.e. who are not regarded as potential supporters of terrorism themselves, are only of interest to the extent that they can provide information about the main target person thought to be associated with terrorism. It would have been imperative that this is reflected in the legal framework. […] 165

3. The scope of the data to be stored pursuant to § 3(1) nos. 1 lit. a and b of the Counter-Terrorism Database Act is not objectionable under constitutional law. However, supplementary provisions are needed with regard to § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act, in respect of certain further details that the provision leaves for the administrative authorities to determine. 166

a) The scope of the basic data set out in § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act, which is made available as non-anonymised information to the participating authorities without qualified thresholds for interference, is not constitutionally objectionable. 167

The scope and informative value of this data can be quite considerable. […] 168

Nevertheless, the provision is compatible with the prohibition of excessive mea- 169

sures. The data is defined in a sufficiently specific manner and, based on an overall assessment, is proportionate in scope. The data is limited to persons who are potentially associated with terrorism (see D IV 2 above), and only used to create a basic profile that allows for a more reliable identification of the persons concerned. While such a profile is indeed informative, it is ultimately limited to external parameters. In view of the importance of combating terrorism, this is not objectionable under constitutional law even if data collected by the intelligence services is included in the database. In this context, it must be taken into account that the data is not newly collected [for the purpose of creating the database], and that the database does not therefore prompt [new] investigation measures with the aim to create a profile with a complete set of basic data, but merely seeks to combine the existing data already held by the different authorities. […]

b) The scope of the extended data to be stored pursuant to § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act is also not objectionable under constitutional law with regard to the prohibition of excessive measures; this data is generally only accessible to the participating authorities in the form of searches that keep the actual data concealed, while direct access to the data in its non-anonymised form is only granted in [acute and exceptional] cases of urgency. However, for certain categories of data to be stored, which are listed in that provision, their actual nature only becomes clear once the authorities have specified them further through abstract and general rules; in this regard, the legislator must ensure that such further determinations made by administrative authorities are comprehensibly documented and published. 170

aa) The categories of data to be stored in the database pursuant to sub-clauses aa to ff, jj, ll, mm, oo, pp and qq of § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act are not objectionable under constitutional law. 171

(1) The categories of data to be entered into the counter-terrorism database pursuant to these sub-clauses are sufficiently specific; they do not require, as another step before they can be applied, further determination through abstract and general rules by the administrative authorities. The scope of the obligation to store data is directly ascertainable from the law, and its application in practice can directly be reviewed by oversight bodies and, as the case may be, by the courts. […] 172

(2) The categories of data to be entered into the database are compatible with the prohibition of excessive measures, including in respect of their scope and informative value. 173

Nevertheless, it must be noted that the potential informative value of this data is extensive. […] 174

Yet again, it must also be taken into account that the provisions do not authorise the collection of new data, but provide only for a combining of data already held by the different authorities. Most importantly, the weight of interference must be balanced 175

against the exceptionally weighty public interest in the effective investigation of and fight against international terrorism (see D III 3 b above). Given the enormous dangers associated with terrorist crime for the most high-ranking legal interests of individuals and for the legal order as a whole, the combined storage of this data for the legislative aims pursued is compatible with the prohibition of excessive measures in an overall assessment.

[…] 176-177

bb) The categories of data to be stored in the database pursuant to sub-clauses gg, hh, ii, kk, nn of § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act are compatible with the Constitution, too. However, the legislator must ensure that the administrative authorities document and publish the rules required for further specifying the application of these categories in practice. 178

(1) These sub-clauses satisfy the requirement of specificity. 179

It is true that these provisions require further determinations [by the administrative authorities] to specify their substantive contents, and that individuals cannot conclusively infer from the provisions themselves what information is actually stored in the database based thereon. […] According to the legislative intent, the detailed determination of the information to be included in the database is not meant to conclusively derive from the statutory provisions as such, but only from further specifying determinations made by the security authorities through abstract and general rules. In a first step, the authorities must define the information to be included in the order establishing the database [issued by the Federal Criminal Police Office in consultation with the other authorities and with governmental approval] pursuant to § 12 no. 3 of the Counter-Terrorism Database Act, and, in another step, in a standardised computer programme (cf. BTDrucks 16/2950, p. 17). Despite the strictly worded data storage obligations laid down in § 3(1) of the Counter-Terrorism Database Act, the legislator evidently did not intend to conclusively determine in that provision that all information potentially falling into the statutory categories listed there was in fact to be included in the database. Rather, it wanted to leave this decision to the authorities. 180

Despite this broad wording and need for further determination, the provisions satisfy the requirements of legal clarity and specificity in the overall framework of the database. The requirement of specificity does not from the outset preclude the use of indeterminate legal concepts (*unbestimmte Rechtsbegriffe*) (BVerfGE 118, 168 <188>). However, the legislator must draft laws as specifically as possible, taking account of the particular nature of the underlying subject matter and the purposes pursued (BVerfGE 78, 205 <212>; cf. also BVerfGE 110, 370 <396>; 117, 71 <111>). […] 181

The counter-terrorism database primarily serves to facilitate requests for information among various security authorities, and to provide easier access to decentralised intelligence, including unconfirmed findings, from other authorities in order to render 182

counter-terrorism measures more effective. In this context, it is not reasonable to demand that the legislator lay down a more precise statutory definition of the data to be stored in the database. […] It is not objectionable with regard to the principle of specificity that the legislator works with an open definition of the relevant data categories, which requires further specifying determinations at the level of implementation, and then sets out a tiered procedure for how the authorities are to carry out these determinations in practice in order to further specify and limit the information that will actually be entered into the database according to technical criteria. Such specifying decisions, even if they entail abstract and general determinations that are of considerable importance, are not a task that is necessarily incumbent upon the legislator itself. Rather, in a state order based on the separation of powers, it is not objectionable under the principle of the rule of law to leave these determinations to the executive. The decisive factor in the present case is that the legislator has not granted a blanket authorisation to the authorities, but has described the relevant data categories in a way that provides a sufficient basis for further determinations [at the level of implementation]. […]

(2) To compensate for the broad wording of the provisions and the need for their further determination [at the level of implementation], the legislator must ensure that the security authorities comprehensibly document and publish their specifying and standardising determinations that will ultimately govern the application of the provisions in the individual case. 183

[…] 184

The current statutory framework does not fully satisfy these requirements […]. 185

[…] The Counter-Terrorism Database Act does not in a sufficiently clear manner impose on the security authorities an obligation to document and publish their determinations that specify the indeterminate legal concepts set out in § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act. Even the fact that the data to be entered into the database is to be further specified at the level of implementation by means of a standardised IT-based catalogue cannot be directly derived from the law itself, but is revealed only in the legislative materials. […] 186

The current statutory framework does not satisfy the requirements for a design in accordance with the rule of law. If the legislator wishes to keep the indeterminate legal concepts in § 3(1) no. 1 lit. b gg, hh, ii, kk, nn of the Counter-Terrorism Database Act, it must enact supplementary provisions that require the security authorities to document and publish, in a comprehensible manner, how they have specified the data categories as provided for in the statutory framework. 187

(3) With regard to their content, the categories of data to be included in the database pursuant to § 3(1) no. 1 lit. b gg, hh, ii, kk, nn of the Counter-Terrorism Database Act are compatible with the prohibition of excessive measures. Although this data may in some cases reveal highly personal circumstances – especially when linked with other 188

stored data –, the legislator is within its leeway to design given that the database is for limited uses only and given the importance of counter-terrorism (see D III 3 a bb, b above).

This also applies to the data to be stored on ethnic origin and religious affiliation pursuant to § 3(1) no. 1 lit. b gg and hh of the Counter-Terrorism Database Act. However, particularly stringent requirements apply in this regard, given that special constitutional guarantees protect against discrimination on these grounds under Art. 3(3) of the Basic Law, and religious affiliation is specifically protected from an obligation to disclose it by Art. 140 of the Basic Law and Art. 136(3) of the Weimar Constitution. […] However, in view of the importance accorded to effective protection against terrorism, it is not ruled out from the outset that this type of data, too, may be included in the database. Nevertheless, the Constitution requires restraint. This can be accommodated by ensuring that such information is only included for identification purposes. 189

cc) The possibility of free text entries pursuant to § 3(1) no. 1 lit. b rr of the Counter-Terrorism Database Act is also compatible with the prohibition of excessive measures. It does not amount to a blanket authorisation for arbitrary inclusion of further information in the database; rather, it allows authorities to provide additional comments and assessments which cannot be reflected otherwise due to the standardisation and categorisation of the entries. […] 190

4. The regime governing data use is not compatible with the prohibition of excessive measures in every respect. 191

a) Nevertheless, § 3(1) no. 1 lit .a of the Counter-Terrorism Database Act, which allows for the request and use of basic data, is not objectionable under constitutional law. 192

aa) § 5(1) first and second sentence of the Counter-Terrorism Database Act provides the participating authorities with direct access to this data in its non-anonymised form. Authorities can both search for names and search in one or more of the categories listed in § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act in order to identify persons not yet known to them. In the event of a match, access is then granted to the entire set of basic data stored on these persons. In this respect, § 5(1) first sentence of the Counter-Terrorism Database Act does not establish qualified thresholds for these measures constituting interferences. According to this provision, searches are generally permissible if they are necessary for the relevant authority's tasks regarding the investigation of and fight against international terrorism. […] 193

The participating authorities can thus make extensive information requests and searches in the basic data. Yet this does not mean that these powers are unlimited. In particular, one limitation is that § 5 of the Counter-Terrorism Database Act only permits individual searches, but no profiling, bulk searches and searches for general 194

links between persons by combining data fields. Thus, the provision requires a specific investigation basis prompting the search in the individual case. Moreover, every request for information is subject to the requirement of necessity, which must be fully substantiated and assessed in each individual case. […]

bb) Despite the remaining wide range of possible ways in which authorities can consult the database, resulting in particular from the absence of limiting thresholds, the statutory framework is compatible with the principle of proportionality in this regard. The provisions governing data use are decisive here. Pursuant to § 6(1) first sentence of the Counter-Terrorism Database Act, the accessed data may only be used to identify persons that are relevant to an investigation, and to prepare individual data transfer requests to the authority holding the relevant information. The authorities are not allowed to extract any further information from this data and directly use it as the basis for investigations or [other operational] actions. They may only obtain such information in a further step [by filing an individual information request] under the applicable specific legislation. […] In relation to the basic data pursuant to § 3(1) lit. a of the Counter-Terrorism Database Act, such a limited, preliminary form of data sharing is not objectionable under the principle of proportionality, given the great importance of protection against terrorism. To that extent, § 5(1) first and second sentence and § 6(1) first sentence of the Counter-Terrorism Database Act are constitutional. 195

b) § 5(1) first and third sentence of the Counter-Terrorism Database Act allows for searches in the extended data pursuant to § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act; this is compatible with the prohibition of excessive measures to the extent that is concerns searches for specific names. 196

§ 5(1) first sentence of the Counter-Terrorism Database Act permits search requests in respect of all data included in the counter-terrorism database, and therefore also searches in the extended data. § 5(1) third sentence of the Counter-Terrorism Database Act provides that if a search for the name of a person yields a match in the extended data, the authority does not get access to the extended data as such, but only receives a notification that there is a positive match, together with information on which authority holds the relevant data and the file reference [under which the data is stored there]. Access to the extended data as such is only possible if the authority holding the information releases it following an individual transfer request subject to the applicable specific legislation (§ 5(1) third and fourth sentence of the Counter-Terrorism Database Act). […] 197

c) By contrast, the statutory authorisation to carry out searches based on criteria [other than name] in the extended data that provide the authority consulting the database not just with information on how and where to request the [extended] data in the event of a match, but also with direct access to the corresponding basic data pursuant to § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act, is not compatible with the prohibition of excessive measures. In that respect, § 5(1) second sentence no. 1 lit. a of the Counter-Terrorism Database Act is unconstitutional. 198

The informative value of the extended data pursuant to § 3(1) no. 1 lit. b of the Counter-Terrorism Database Act is extensive, and can include highly personal information as well as data that pieces together the biographical background of the data subject (see D IV 3 b aa (2) above). Based on proportionality considerations, access to this type of information must therefore be restricted to a significantly greater degree than access to basic data pursuant to § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act. Accordingly, the law generally only authorises searches that keep the extended data itself concealed [from the authority consulting the database], and makes transfer of the non-anonymised data subject to the transfer provisions under the respective statutory regimes applicable in the specific case. Yet in the event that searches in the extended data yield a match, the law also grants direct access to the corresponding basic data in its non-anonymised form; as a result, it lifts the aforementioned access restriction for searches based on criteria [other than name], i.e. reverse searches, to a significant extent. […] Thus, authorities can consult the database by searching for one or several criteria – for example, by searching for persons with a certain religious affiliation and training who frequent a certain meeting place (cf. § 3(1) no. 1 lit. b hh, jj, nn of the Counter-Terrorism Database Act) – and thereby obtain, in the event of a match, not just the information which other authorities hold relevant information, but all names and addresses and all other information listed in § 3(1) no. 1 lit. a of the Counter-Terrorism Database Act about all persons matching the search criteria. 199

Such far-reaching data use does not take sufficient account of the fact that the extended data are substantive in scope. […] The design of the provisions governing use of the database must ensure that, if a search in the extended data yields a match, only the file reference and the authority holding the [concealed] data are displayed, but not the corresponding basic data. 200

d) This notwithstanding, there are no constitutional objections to allowing the [direct] use of extended data in urgent cases pursuant to § 5(2) and § 6(2) of the Counter-Terrorism Database Act, even in the context of reverse searches (see c above). 201

It is true that this constitutes the broadest possible use of the data combined in the counter-terrorism database. In addition to basic data access, it entails direct access to all extended data in its non-anonymised form, and therefore allows [the authority consulting the database] to use the data not just to prepare further transfer requests, but also to directly carry out counter-terrorism measures for instance if the data is used for assessing a danger as the basis for further operational action (§ 6(2) of the Counter-Terrorism Database Act). As this deviates from the principle of separation of police and intelligence data, it amounts to a particularly serious interference (see D III 3 a aa, bb (3) above). 202

The statutory prerequisites for such use are, however, sufficiently narrow to justify the interference. The data may be accessed and used only to protect particularly weighty legal interests – which primarily concerns the protection of life, limb, health 203

or liberty of the person. […] To the extent that the provision additionally lists assets of substantial value as protected interests, it clarifies that this does not entail protection of property or material assets as such, but only applies to assets “the preservation of which is required in the public interest” (§ 5(2) first sentence of the Counter-Terrorism Database Act). In the context of protecting against terrorism, this means significant infrastructure facilities or other sites that are vital for society. The provision also sets out high thresholds for carrying out the measures. It requires a present danger to protected interests, the existence of which must be established not just based on mere indications, but based on specific substantiating facts. The data may then only be accessed and used if this is absolutely necessary and if the relevant data could not be retrieved in time through an individual transfer request. Moreover, direct access to the data is subject to procedural safeguards. […]

5. The principle of proportionality also gives rise to requirements regarding transparency, individual legal protection and administrative oversight. Given the purpose and design of the database, the Counter-Terrorism Database Act only ensures transparency regarding information sharing to a limited extent, thus allowing affected persons only limited possibilities of legal protection; thus, its application is essentially overseen by the data protection officers. This is compatible with the Basic Law provided that the constitutional requirements regarding effective oversight are observed. 204

a) As regards the storage and use of personal data by state authorities in the exercise of their functions, the legislator must also satisfy requirements regarding transparency, legal protection, and administrative oversight in consideration of proportionality aspects (cf. BVerfGE 125, 260 <325 *et seq*.>). 205

[…] 206-207

b) The Counter-Terrorism Database Act contains few provisions for ensuring transparency and individual legal protection. In essence, it only recognises rights to information [on the part of data subjects], which are limited in their effectiveness by procedural law and substantive restrictions. Yet in view of the purpose and design of this database, this is not objectionable. 208

aa) To ensure transparency, the Counter-Terrorism Database Act primarily provides for rights to information based on the Federal Data Protection Act (§ 10(2) of the Counter-Terrorism Database Act). However, these rights are subject to restrictions and, in part, considerable procedural hurdles. Yet in view of the purpose pursued by and the function of the Counter-Terrorism Database Act, these limited information rights satisfy the constitutional requirements. 209

[…] 210-212

bb) Other than that, the Counter-Terrorism Database Act neither sets out a requirement that data use be in principle carried out overtly, nor a requirement of prior judicial authorisation (*Richtervorbehalt*) nor requirements to notify the affected persons *ex post* beyond the notification requirements already contained in other legislation. 213

Thus, the Act lacks important instruments for ensuring the proportionality of data use. Yet this is justified under constitutional law given the purpose of the counter-terrorism database. It mainly serves to facilitate requests for information in order to prepare further investigation measures in the context of protection against international terrorism. It is evident that this type of investigations cannot generally observe the principle of transparency. As regards the counter-terrorism database, prior judicial authorisation can also not be considered a viable instrument mandated under constitutional law. Given that the statutory framework does not conclusively define all details of the powers set out in § 5(1) of the Counter-Terrorism Database Act, and given that data access pursuant to § 5(2) of the Counter-Terrorism Database Act concerns cases of urgency requiring an expedited procedure, a requirement to obtain prior judicial authorisation would be ineffective for the most part. […]

c) Since the Counter-Terrorism Database Act can only ensure transparency of data processing and individual legal protection to a very limited extent, guaranteeing effective administrative oversight is all the more significant. Therefore, the principle of proportionality places more stringent requirements on the effective design of such an oversight regime both at statutory level and at the level of implementation. 214

aa) Ensuring effective oversight primarily requires oversight bodies equipped with effective powers at both the federal and *Land* level, such as the data protection officers under current law. It is also necessary to comprehensively document any access to and modifications of the data records. In this regard, technical and organisational arrangements must ensure that the data is available to the data protection officers in a form that allows them to conduct effective audits, and that the required documentation provides sufficient information to match the data with the process to be audited. 215

Given the nature of the counter-terrorism database as a joint database used both by federal and *Land* authorities, it must be ensured that effective oversight of the database does not stand back behind optimising data sharing due to uncertainties about the division of competences in the federal order. […] Regarding the relationship between different oversight authorities, it must be ensured that effective oversight is exercised in respect of data obtained by measures taken under the Article 10 Act [i.e. surveillance measures restricting the privacy of telecommunications under Art. 10 of the Basic Law] – which is of particular importance given that a significant amount of the data stored in the database is contributed by the Federal Intelligence Service. If the legislator provides for cooperation among security authorities in the form of information sharing, it must also allow for cooperation among oversight authorities to uphold data protection. 216

Since administrative oversight must compensate for the weak level of individual legal protection, it is particularly significant that audits be performed regularly at intervals not exceeding approximately two years. This must be taken into account when allocating resources to the oversight authorities. 217

bb) […] 218-220

d) In order to ensure transparency and oversight, the legislator must enact statutory reporting obligations. 221

Under the Counter-Terrorism Database Act, the data is largely stored and used without the knowledge of affected persons or the public; rights to information can only counteract this to a limited extent. Furthermore, effective judicial review is not sufficiently possible. Therefore, the law must ensure regular reports by the Federal Criminal Police Office to Parliament and the public on what data is included in the counter-terrorism database and how it is used. […] 222

6. There are no constitutional objections regarding the deletion arrangements pursuant to § 11(2) and (4) of the Counter-Terrorism Database Act. According to this provision, the maximum duration for which data may be stored depends on the deletion periods set out in the specific legislation governing the respective source data which is entered into the database. This approach is sensible, and it is also tenable under constitutional law. 223

V.

To the extent that the challenged provisions allow data obtained through interferences with the privacy of telecommunications or with the fundamental right to the inviolability of the home to be included in the database, they violate Art. 10(1) and Art. 13(1) of the Basic Law. 224

1. Data collected through interferences with the fundamental rights under Art. 10(1) and Art. 13(1) of the Basic Law is generally subject to more stringent requirements, due to the special protection afforded by these fundamental rights. According to the case-law of the Federal Constitutional Court, these more stringent requirements continue to apply to any later transfer and change in purpose of data thus obtained. For instance, the statutory threshold for the transfer of data obtained through the surveillance of private homes for criminal proceedings may not be lower than the threshold applicable to similar interferences for public security purposes, since a change in purpose may not be used to circumvent restrictions set by fundamental rights regarding the use of certain investigation methods (cf. BVerfGE 109, 279 <377 and 378>; cf. also BVerfGE 100, 313 <389 and 390, 394>). Likewise, the sharing of telecommunications data, which could only be obtained by the sharing authority subject to particularly stringent requirements, is only permissible if it serves tasks that would [hypothetically] have justified direct access to this data by the receiving authority (cf. BVerfGE 125, 260 <333>; similarly already BVerfGE 100, 313 <389 and 390>; 109, 279 <375 and 376>; 110, 33 <73 and 74>). For the same reasons, data stemming from serious interferences with Art. 10(1) or Art. 13(1) of the Basic Law must be labelled accordingly. Making such data identifiable serves to ensure that the specific restrictions on the use of this data are observed even in the event that the data is transferred to other authorities. 225

2. Full and unrestricted inclusion in the counter-terrorism database of data obtained 226

through interferences with Art. 10(1) and Art. 13(1) of the Basic Law is not compatible with these requirements; the same applies to data obtained through interferences with the fundamental right to protection of the confidentiality and integrity of information technology systems under Art. 2(1) in conjunction with Art. 1(1) of the Basic Law (cf. BVerfGE 120, 274 <302 and 303>), a violation of which was not asserted by the complainant in the present proceedings. Where data is protected by these fundamental rights, it may generally only be collected subject to strict standards, which require, for example, higher statutory thresholds for carrying out measures constituting interferences with these rights, such as the requirement of a qualified danger or a qualified suspicion, a danger to exceptionally significant legal interests, or the prosecution of particularly serious criminal acts. […]

3. In the oral hearing, the Federal Government stated that, in the future, such data would only be stored in a concealed manner pursuant to § 4 of the Counter-Terrorism Database Act. This does not, however, lead to a different result in the present proceedings given that no such limitation can be inferred from the Counter-Terrorism Database Act itself. […] 227

This notwithstanding, if the statutory framework were to always require concealed storage of such data pursuant to § 4 of the Counter-Terrorism Database Act, it would be constitutional with regard to the principle of proportionality. With such a design, the statutory framework would ensure that the corresponding information can only be accessed in accordance with the transfer provisions set out in the applicable specific legislation. Those provisions, in turn, can ensure both qualified thresholds for interference, as required under constitutional law, and the protection of sufficiently weighty legal interests. […] 228

E.

I.

Despite the fact that the challenged provisions are in part unconstitutional, they are not declared void but incompatible with the Basic Law. […] 229

A mere declaration of incompatibility, combined with an order to temporarily continue the application of unconstitutional provisions, can be issued if the immediate invalidity of the objectionable provision would eliminate the statutory basis for the protection of exceptionally significant public interests, and if a balancing of these interests against the affected fundamental rights requires that the interference be tolerated for a transitional period (BVerfGE 109, 190 <235 and 236>). This is the case here. […] 230

[…] 231-232

II.

The decision is unanimous with regard to part C; with regard to other parts, there were partial dissents. […] 233

Kirchhof Gaier Eichberger

Schluckebier Masing Paulus

Baer Britz

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

Zitiervorschlag BVerfG, Beschluss 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