1. ------IND- 2015 0288 D-- EN- ------ 20150707 --- --- PROJET

Governmental draft

of the Federal Ministry of Justice and Consumer Protection

Draft Act introducing a storage obligation and a maximum retention period for traffic data

A. Problem and objective

Traffic data constitutes an important tool for the public authorities when investigating criminal offences and protecting against threats. Traffic data within the meaning of § 96 of the Telecommunications Act [German designation: TKG] is understood to mean data which accumulates through telecommunications, e.g. the call number of the participating connections as well as the time and place of a telephone call. It is not an issue of the content of the telecommunication but of whether the telecommunication has taken place at all and, if so, when. At present, the criminal prosecution authorities may collect data from telecommunications companies on the basis of § 100g of the Code of Criminal Procedure [German designation: StPO] where there are initial grounds for suspicion and a corresponding judicial order exists. This only applies, however, to data which accumulates in the future and to data that is still being stored at the time of the inquiry, for example, because it is still needed for commercial reasons. The storage period varies between individual companies, ranging from just a few days to many months. It therefore comes down to chance whether traffic data are still available or not at the time of the inquiry. This leads to loopholes during the prosecution of criminal offences and while protecting against threats and may, in a given case, lead to criminal investigations failing because further investigative approaches are not available.

This state of affairs is difficult to reconcile with the importance befitting effective prosecution. The Federal Constitutional Court has repeatedly highlighted the requirement under constitutional law for effective prosecution, emphasised the interest in ascertaining the truth in criminal proceedings as fully as possible, and labelled the effective investigation of especially serious criminal offences as an important mandate of a constitutional community (Federal Constitutional Court Decisions 129, 208 <260> with further references). In order to change this state of affairs, it is necessary to introduce a statutory obligation for the providers of publicly available telecommunications services to store traffic data. However, a corresponding provision shall be subject to strict requirements regarding the scope of the stored data and data use on account of the infringements of fundamental rights associated with it. This provision must be limited to what is strictly necessary. A high standard must be prescribed in a legally transparent and binding manner in relation to data security.

This was not the case as regards the previous provisions regarding the introduction of a storage obligation for crime prevention and for protecting against threats at both a European and national level. As a result, in its judgment of 2 March 2010 (Federal Constitutional Court Decisions 125, 260), the Federal Constitutional Court declared §§ 113a and 113b of the Telecommunications Act, and also § 100g(1) sentence 1 of the Code of Criminal Procedure, insofar as traffic data as per § 113a of the Telecommunications Act could be collected in accordance with these provisions, to be invalid on account of an infringement of Article 10(1) of the Basic Law [German designation: GG] and thereby repealed as a result the definitive provisions for transposing Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly

available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105 of 13 April 2006, p. 54). On 8 April 2014, the Court of Justice of the European Union declared Directive 2006/24/EC to be invalid (associated cases C-293/12 and C-594/12, EuZW [European Journal of Economic Law] 2014, 459) on account of the fact that it restricted the basic rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union to a disproportionate extent.

B. Solution

A provision is being established regarding the temporary storage of traffic data in connection with crime prevention and for protecting against threats. This provision is designed to shape in a lawful manner the encroachment into telecommunications secrecy arising from Article 10 of the Basic Law and the fundamental rights to data protection under Article 7 (respect for privacy) and Article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union on the grounds of effective prosecution. It does so as a result of the fact that although provision is made for an obligation on the part of the providers of telecommunications services to store the specifically designated traffic data for a limited period, collection of the data by government agencies is only made possible under very strict conditions. The intensity of the encroachment is reduced clearly as a result of a markedly reduced volume of data (no compulsory storage of data by electronic mail services) and a very brief retention period (four or ten weeks) compared with the previous arrangement.

With respect to the collection of data for the purpose of prosecuting particularly serious criminal offences, the reworded § 100g of the Draft Code of Criminal Procedure makes provision for powers scaled according to the intensity of the encroachment which differentiate between the traffic data stored by the providers of publicly available telecommunications services for commercial purposes (§ 100g(1) of the Draft Code of Criminal Procedure) and that traffic data stored on a compulsory basis in accordance with §§ 113a *et seq.* of the Draft Telecommunications Act (§ 100g(2) of the Draft Code of Criminal Procedure). In accordance with the stipulations under fundamental law, the traffic data to be stored on a compulsory basis shall only be collected under very strict conditions, in particular for the purpose of prosecuting particularly serious criminal offences indicated under § 100g(2) of the Draft Code of Criminal Procedure, which also have to be taken seriously in a given case. Stored location data may only be collected under the same strict conditions. Furthermore, the requirements pertaining to a radio cell inquiry are defined more precisely in order to ensure that proportionality is maintained when collecting this data as well.

The need to ensure adequate protection under criminal law of information systems and the data stored in them against attacks and illicit access contrasts with the necessity of facilitating effective prosecution in a society increasingly characterised by information and communication technology. This protection must also be directed against acts constituting the offence by means of which tracked or intercepted data, or data unlawfully acquired in another way, is handled and so that the encroachment on the formal right of disposal of his data on the part of the beneficiary, which is effected by means of the prior offence, is continued and consolidated. The currently applicable provisions under criminal law against dealing with data acquired illegally are inadequate and have loopholes in terms of protection. The draft therefore makes provision for the introduction of a new criminal offence of receiving stolen data (§ 202d of the German Criminal Code). According to this, a party is to be liable to prosecution when he makes available for himself, or to someone else, data which is not publicly available which another party has acquired as a result of an unlawful act, when he relinquishes said data to another party, or when he disseminates the data or makes it available in another way, in order to make money for himself or a third party or to injure someone else.

C. Alternatives

None.

D. Budget expenditure without compliance costs

None.

E. Compliance costs

E.1 Compliance costs for citizens

No compliance costs shall arise for citizens.

E.2 Compliance costs for businesses

Additional expense shall arise for the telecommunications companies in question as a result of fulfilment of the storage obligation provided for in § 113b of the Draft Telecommunications Act and the associated – on account of the stipulations of the Federal Constitutional Court - unavoidable provisions concerning use of the data, the guaranteeing of data security and data quality, the logging of access to the data and the inclusion of certain information in the security concept to be drawn up.

Additional expense shall also be incurred as a result of the obligation to transmit traffic data associated with the storage obligation provided for in § 113b of the Draft Telecommunications Act in accordance with § 100g(2) of the Draft Code of Criminal Procedure and the obligation to exchange information regarding inventory data as per § 100j of the Draft Code of Criminal Procedure.

This expense can only be estimated: According to the German trade association BITKOM, the obligation introduced in 2007 regarding the retention of data resulted, in the case of the telecommunications companies organised therein, in necessary investment in the amount of approximately EUR 75 million. On top of this, there were annual operating costs amounting to tens of millions. In contrast, the *Verband der deutschen Internetwirtschaft eV* [German Internet Association] (eco) stated that in connection with the retention of data in the form originally specified by the European Union, the digital economy has invested in excess of EUR 300 million in the necessary technology. Additional costs may arise as a result of the heightened data security requirements and changes due to technical developments. On the other hand, the companies should be able, at least in part, to draw on the investment already undertaken. In terms of specific companies, at that time, investment totalling from EUR 3 to 9 million was required each time. Since the storage obligation affects all telecommunications companies equally, approx. 1 000 companies are affected. As regards the anticipated costs, a distinction must be made between the capital expenditure associated with first-time set-up and the running costs relating to the constant updating of the safeguarding measures. Since the situation may take shape very differently with the individual companies, the level of expense cannot be quantified at present.

The expenditure which shall arise in connection with the transmission of traffic data and the exchanging of information regarding inventory data are reimbursed in accordance with § 23 of the Court Allowances Act [German designation: JVEG]. In addition, the draft makes provision for a compensation scheme regarding the investment and, as appropriate, increased operating costs necessary for fulfilling the storage obligations as

per §§ 113b *et seq.* of the Draft Telecommunications Act in the event that the costs incurred could choke individual companies.

Of which bureaucratic costs arising from obligations to provide information

The draft introduces four new obligations to provide information within the meaning of the Act instituting a National Regulatory Council.

E.3 Compliance costs for administration

As a result of the amendment of the provisions of the Telecommunications Act in Article 2, the Federal Network Agency shall incur enforcement costs, to be subdivided into real investment and personnel costs. This - on account of the stipulations of the Federal Constitutional Court in its judgment relating to the retention of data unavoidable - additional expense shall accrue, *inter alia*, as a result of the obligation pursuant to § 113f of the Draft Telecommunications Act to draw up a catalogue of requirements, review this on a continuous basis and adapt it immediately as required. Moreover, increased monitoring expenditure shall result from the obligation to store traffic data in the context of supervision under § 115 of the Telecommunications Act and the application of the new offences which could result in a fine. These new tasks shall result in a requirement for 25 permanent posts/jobs involving annual personnel costs in the amount of EUR 2.9 million on the part of the Federal Network Agency. In addition, one-off equipment costs in the amount of EUR 150 000 shall be incurred in the first year. Additional costs shall also be incurred by the Federal Data Protection and Freedom of Information Commissioner as well as by the Federal Office for Information Technology Security.

The impact of the compensation scheme in § 113a(2) of the Draft Telecommunications Act is still to be assessed. Of the approximately 1 000 providers of publicly available telecommunications services in existence, 20 are so big that they account for 98 % of the market, while the remainder are small- and medium-sized companies which will presumably frequently plead undue hardship. This can only happen, however, if the corresponding catalogue of requirements (§ 113f of the Draft Telecommunications Act) has been drawn up by the Federal Network Agency.

A decision shall be taken in the context of future budgetary procedures regarding the financing of the budgetary burden associated with the draft legislation.

No compliance costs shall be incurred by the municipalities.

F. Further costs

The traffic data inquiry does not constitute a new investigative tool. It is anticipated that the judiciary shall not incur any appreciable costs since it is presumed that the level of inquiries will be the same as before but will lead to better outcomes. The cost lump sums to be granted in accordance with the Court Allowances Act shall put a strain on the Federal State budgets. It is not anticipated, however, that this burden shall be substantially higher than is the case with the existing provisions.

As a result of the introduction of a new criminal offence of receiving stolen data (§ 202d of the Draft German Criminal Code), the Federal State budgets shall incur procedural and enforcement costs, the precise level of which cannot be quantified in greater detail.

In any event, the Federal Government shall incur a limited amount of additional expenditure. Any increased demand for equipment and personnel can be offset within

existing capacity and available funds and must be balanced, in terms of funds and job numbers, in the respective detailed plan 07 (detailed plan of the Federal Ministry of Justice and Consumer Protection).

Governmental draft of the Federal Ministry of Justice and Consumer Protection

Draft Act introducing a storage obligation and a maximum retention period for traffic data

dated …

The *Bundestag* has adopted the following Act:

Article 1

Amendment of the Code of Criminal Procedure

The Code of Criminal Procedure, in the version published on 7 April 1987 (Federal Law Gazette I pp. 1074, 1319), as last amended by …, is amended as follows:

1. In the Table of contents, the following entries are inserted after the statement relating to § 101:

   "§ 101a Adjudication, data identification and analysis, obligations to notify when collecting traffic data

   § 101b Statistical recording of the collection of traffic data".

2. § 100g is worded as follows:

"§ 100g

Collection of traffic data

(1) If specific facts create the suspicion that a person, as perpetrator or accessory,

1. has committed a criminal offence which, even in an individual case, is of substantial importance, in particular a criminal offence listed in § 100a(2) or, in cases in which such attempt constitutes an offence, has attempted to commit such an offence, or has committed a criminal offence preparatory thereto, or

2. has committed an offence by means of telecommunications,

then traffic data (§ 96(1) of the Telecommunications Act) may be collected if this is necessary for the purpose of investigating the facts of the case and the collection of the data are in a reasonable proportion to the importance of the matter. In the case of sentence 1 point 2, the measure is only permitted if investigating the facts of the case in another way would be futile. Location data may only be collected in accordance with this paragraph in relation to traffic data which accumulates in future or in real time, and only in the case of sentence 1 point 1, if this is necessary for the purpose of investigating the facts of the case or for establishing the whereabouts of the suspect.

(2) If specific facts create the suspicion that a person, as perpetrator or accessory, has committed one of the particularly serious criminal offences indicated in sentence 2 or, in cases in which such attempt constitutes an offence, has attempted

to commit such an offence and, in a given case, the offence also has to be taken particularly seriously, the traffic data stored in accordance with § 113b of the Telecommunications Act may be collected if investigating the facts of the case or establishing the whereabouts of the suspect in another way would be futile or considerably more difficult and the collection of the data are in a reasonable proportion to the importance of the matter. The following constitute particularly serious criminal offences within the meaning of sentence 1:

1. under the German Criminal Code:

   a) criminal offences of betrayal of peace, sedition, endangering the democratic rule of law, treason or endangering external security in accordance with §§ 80, 81, 82, 89a, as per § 94, § 95(3) and § 96(1), in each case also in conjunction with § 97b, as well as in accordance with § 97a, § 98(1) sentence 2, § 99(2) and § 100 and § 100a(4),

   b) a particularly serious case of a breach of the peace in accordance with § 125a, forming a criminal organisation as per § 129(1), in conjunction with paragraph 4 clause 2, and forming terrorist organisations in accordance with § 129a(1), (2), (4), (5) sentence 1 option 1, in each case also in conjunction with § 129b(1),

   c) crimes against sexual self-determination in the cases of § 176a, § 176b, § 177(2) sentence 2 point 2 and § 179(5) point 2,

   d) the dissemination, acquisition and possession of writings constituting child pornography in the cases of § 184b(2) and § 184c(2),

   e) murder and manslaughter in accordance with §§ 211 and 212,

   f) criminal offences against personal liberty in the cases of § 234, § 234a(1) and (2), § 239a and § 239b and trafficking in human beings for sexual exploitation and for the purpose of exploiting labour as per § 232(3), (4) or (5) or § 233(3), where these constitute crimes each time,

   g) serious gang theft as per § 244a(1), aggravated robbery as per § 250(1) or (2), robbery involving the death of the victim as per § 251, extortion in accordance with § 255 and a particular serious case of blackmail as per § 253 under the conditions mentioned in § 253(4) sentence 2, receiving stolen goods for gain as per § 260a(1), a particularly serious case of money laundering and the concealment of unlawfully obtained assets as per § 261 under the conditions mentioned in § 261(4) sentence 2,

   h) crimes involving danger to the community in the cases of § 306 to § 306c, § 307(1) to (3), § 308(1) to (3), § 309(1) to (4), § 310(1), § 313, § 314, § 315(3), § 315b(3) and §§ 316a and 316c,

2. under the Residence Act:

   a) trafficking in aliens in accordance with § 96(2),

   b) trafficking resulting in death or commercial and organised trafficking as per § 97,

3. under the Foreign Trade Act:

   criminal offences in accordance with § 17(1) to (3) and § 18(7) and (8),

4. under the Narcotics Act:

   a) a particularly serious criminal offence in accordance with § 29(1) sentence 1 points 1, 5, 6, 10, 11 or 13 and paragraph 3 under the condition mentioned in § 29(3) sentence 2 point 1,

   b) a criminal offence as per § 29a, § 30(1) points 1, 2 and 4, § 30a,

5. under the Precursor Monitoring Act:

   a criminal offence in accordance with § 19(1) under the conditions mentioned in § 19(3) sentence 2,

6. under the War Weapons Control Act:

   a) a criminal offence as per § 19(2) or § 20(1), in each case also in conjunction with § 21,

   b) a particularly serious criminal offence in accordance with § 22a(1), in conjunction with paragraph 2,

7. under the International Criminal Code:

   a) genocide as per § 6,

   b) crimes against humanity as per § 7,

   c) war crimes as per §§ 8 to 12,

8. under the Weapons Act:

   a) a particularly serious criminal offence in accordance with § 51(1), in conjunction with paragraph 2,

   b) a particularly serious criminal offence in accordance with § 52(1) point 1, in conjunction with paragraph 5,

(3) The collection of all the traffic data which has accrued in a radio cell (radio cell inquiry) is only permitted

1. if the conditions under paragraph 1 sentence 1 point 1 are satisfied,

2. If the data collection is in a reasonable proportion to the importance of the matter and

3. if the investigation of the facts of the case or the establishment of the whereabouts of the suspect in another way would be futile or considerably more difficult.

Recourse may only be made to traffic data stored in accordance with § 113b of the Telecommunications Act in relation to a radio cell inquiry under the conditions laid down in paragraph 2.

(4) Traffic data collection as per paragraph 2, also in conjunction with paragraph 3 sentence 2, which is directed against one of the persons mentioned in § 53(1) sentence 1 points 1 to 5, and which would presumably produce findings concerning which these persons may refuse to give evidence, is not permitted. Knowledge gained nonetheless may not be used. Any records of this must be deleted

immediately. The fact that this knowledge has been obtained and that the records have been deleted must be placed on record. Sentences 2 to 4 shall apply accordingly if, as a result of an investigative measure which is not directed against a person mentioned in § 53(1) sentence 1 points 1 to 5, knowledge is acquired of this person concerning which he or she may refuse to give evidence. § 160a(3) and (4) shall apply accordingly.

(5) If the traffic data are not collected by the provider of publicly available telecommunications services, it shall be determined following the conclusion of the communication process in accordance with the general regulations."

3. In § 100j(2), the words "§ 113(1) sentence 3" are replaced by the words "§ 113(1) sentence 3 and § 113c(1) point 3".

4. § 101 is amended as follows:

a) In paragraph 1, the statement "100c to 100i" is replaced by the statement "100c to 100f, 100h, 100i".

b) Paragraph 4 is amended as follows:

aa) Sentence 1 is amended as follows:

aaa) Point 6 is deleted.

bbb) Points 7 to 12 become points 6 to 11.

bb) In sentence 4, the words "sentence 1 points 2, 3 and 6" are replaced by the words "sentence 1 points 2 and 3".

5. The following §§ 101a and 101b are inserted after § 101:

"§ 101a

Adjudication; data identification and analysis; obligations to notify when collecting traffic data

(6) When collecting traffic data in accordance with § 100g, § 100a(3) and § 100b(1) to (4) shall apply accordingly with the proviso that

1. in the order as per § 100b(2) sentence 2, also the data to be transmitted and the period for which it is to be transmitted must be specified clearly,

2. the party obligated to provide information in accordance with § 100b(3) sentence 1 must also advise as to which parts of the data transmitted by him had been stored in accordance with § 113b of the Telecommunications Act.

In the cases of § 100g(2), also in conjunction with § 100g(3) sentence 2, in deviation from sentence 1, § 100b(1) sentences 2 and 3 shall not apply. In the case of radio cell inquiries pursuant to § 100g(3), in deviation from § 100b(2) sentence 2 point 2, a geographically limited, short-term and sufficiently specific telecommunication shall suffice.

(7) If a measure as per § 100g is ordered or extended, on a case-by-case basis in the explanatory statement, the key considerations in terms of the necessity and appropriateness of the measure, also with respect to the scope of the data to be

collected and the period of time for which it is to be collected, must be stated in particular.

(8) Personal data which has been collected as a result of measures under § 100g must be identified accordingly and evaluated forthwith. When identifying the data, it must be distinguishable whether the data in question was stored in accordance with § 113b of the Telecommunications Act. Once the data has been transmitted to another authority, the latter must maintain this identification. § 101(8) shall apply accordingly to the deletion of personal data.

(9) Usable personal data which has been collected as a result of measures pursuant to § 100g(2), also in conjunction with § 100g(3) sentence 2, may only be used without the consent of the parties involved in the telecommunication in question for the following other purposes and only in accordance with the following stipulations:

1. in other criminal proceedings concerning the investigation of a criminal offence, on which basis a measure as per § 100g(2), also in conjunction with § 100g(3) sentence 2, could be ordered or for establishing the whereabouts of the person accused of committing such a criminal offence,

2. transmission for the purpose of averting specific risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings (§ 113c(1) point 2 of the Telecommunications Act).

The authority which passes on the data shall place on record the fact that the data has been passed on and the purpose behind this. If the data as per sentence 1 point 2 is no longer required to avert the risk or is no longer required for a pre-trial or judicial review of the measures taken to avert the risks, records of this data must be deleted immediately by the authority responsible for protecting against threats. This deletion must be placed on record. If deletion is deferred merely for the purpose of a possible pre-trial or judicial review, the data may only be used for this purpose. It must be blocked in relation to use for other purposes.

(10) If usable personal data which was stored in accordance with § 113b of the Telecommunications Act has been acquired by means of a corresponding police measure, it may only be used in criminal proceedings without the consent of the parties involved in the telecommunication in question for the purpose of investigating a criminal offence, on which basis a measure as per § 100g(2), also in conjunction with paragraph 3 sentence 2, could be ordered or for establishing the whereabouts of the person accused of committing such a criminal offence.

(11) The parties involved in the telecommunication in question must be notified of traffic data collection in accordance with § 100g. § 101(4) sentences 2 to 5 and paragraphs 5 to 7 shall apply accordingly with the proviso that

1. omission of the notification as per § 101(4) sentence 3 requires an instruction from the competent court;

2. in deviation from § 101(6) sentence 1, the deferment of the notification as per § 101(5) sentence 1 always requires an order from the competent court, while a first-time deferment shall be limited to a maximum of 12 months.

§ 101b

Statistical recording of the collection of traffic data

In accordance with § 100b(5), as regards measures as per § 100g, a synopsis shall be drawn up on an annual basis in which the following must be indicated,

3. differentiated according to the measures as per § 100g(1), (2) and (3):

   a) the number of proceedings in which these measures have been carried out;

   b) the number of initial orders by means of which these measures have been arranged;

   c) the number of extension orders by means of which these measures have been arranged;

4. differentiated for the areas of fixed network, mobile and internet services and subdivided each time according to the number of past weeks for which the collection of traffic data were arranged, measured each time from the date of the order:

   a) the number of orders as per § 100g(1);

   b) the number of orders as per § 100g(2);

   c) the number of orders as per § 100g(3);

   d) the number of orders which have proven fruitless in part because the data requested was not available in some cases;

   e) the number of orders which have proven fruitless because no data were available."

6. § 160a is amended as follows:

   a) In paragraph 4 sentence 1, the words "receiving stolen data" are inserted before the words "aiding and abetting,".

   b) In paragraph 5, the statement "§§ 97 and 100c(6)" is replaced by the words "§§ 97, 100c(6) and § 100g(4)".

7. In § 304(4) sentence 2 point 1, the statement "or § 101a(1)“ is inserted after the statement "§ 101(1)".

8. In § 477(2) sentence 4, after the statement "§ 100i(2) sentence 2", a comma and the words "§ 101a(4) and (5)" are inserted.

9. In § 3, § 60 point 2, § 68b(1) sentence 4 point 1, § 97(2) sentence 3, § 102 and § 138a(1) point 3, the words "receiving stolen data," are inserted before every occurrence of the words "aiding and abetting".

Article 2

Amendment of the Telecommunications Act

The Telecommunications Act of 22 June 2004 (Federal Law Gazette I p. 1190), as last amended by ..., is amended as follows:

1. In the Table of contents, the information under §§ 113a and 113b is replaced by the following statements:

2. §§ 113a and 113b are replaced by the following §§ 113a to 113g:

"§ 113a

Obligated parties; compensation

(12) The obligations concerning traffic data storage, data usage and data security in accordance with §§ 113b to 113g relate to providers of publicly available telecommunications services. Any party which provides publicly available telecommunications services but does not itself generate or process all the data to be stored in accordance with §§ 113b to 113g must

1. ensure that the data not generated or processed by the party in the course of providing it service is stored in accordance with § 113b(1) and

2. inform the Federal Network Agency immediately, at its request, regarding who is storing this data.

(13) As regards the unavoidable expenditure incurred by the obligated parties as a result of implementing the stipulations arising from §§ 113b and 113d to 113g, reasonable compensation must be paid if this appears necessary in order to prevent or offset undue hardship. The costs that have actually arisen are decisive in terms of calculating the level of compensation. The Federal Network Agency shall make decisions regarding applications for compensation.

§ 113b

Obligations regarding the storage of traffic data

(1) The parties mentioned in § 113a(1) are obliged to store data in Germany as follows:

1. Data in accordance with paragraphs 2 and 3, for 10 weeks,

2. location data in accordance with paragraph 4, for 4 weeks.

(2) The providers of publicly available telecommunications services shall store

1. the call number or another identifier of the calling and called line, as well as of every additional participating line in the case of call redirection or forwarding,

2. the date and time of the start and end of the call, stating the underlying time zone,

3. information regarding the service used, where various services can be utilised in the context of the telephony service,

4. in the case of mobile telephony services, also

   a) the international prefix of mobile subscribers for the calling and called number,

   b) the international prefix of the calling and the called terminal equipment,

   c) the date and time of the initial activation of the service, stating the underlying time zone, if services have been paid for in advance,

5. in the case of telephony services over the Internet, also the IP addresses of the calling and called number and assigned user IDs.

Sentence 1 shall apply accordingly

1. in connection with the transmission of a short, multimedia or similar message. In this regard, the time the message is sent and received shall supersede the information pursuant to sentence 1 point 2;

2. to unanswered calls or those which have been unsuccessful on account of a network management intrusion if the provider of publicly available telecommunications services stores or logs the traffic data mentioned in sentence 1 for the purposes referred to in § 96(1) sentence 2.

(3) The providers of publicly available Internet access services shall store

1. the IP address assigned to the subscriber for using the internet,

2. an unambiguous call identifier via which internet access is achieved, as well as an assigned user ID,

3. the date and time of the start and end of internet usage under the assigned IP address, stating the underlying time zone.

(4) Where mobile telephony services are used, the radio cell designations which have been used by the calling and called number at the start of the call must be stored. As regards publicly available internet access services, in the case of mobile usage, the designation of the radio cell used at the start of the internet connection must be stored. In addition, data must be retained from which follows the geographical location and the main beam directions of the antennas supplying the respective radio cell.

(5) The content of the communication, data pertaining to websites visited and data from electronic mail services may not be stored on the basis of this regulation.

(6) Data underlying the connections mentioned in § 99(2) may not be stored on the basis of this regulation. This shall apply, *mutatis mutandis*, to telephone connections emanating from the authorities mentioned in § 99(2). § 99(2) sentences 2 to 7 shall apply accordingly.

(7) The data shall be stored so as to enable information requests from the approved authorities to be answered immediately.

(8) The party obligated in accordance with § 113a(1) must delete forthwith the data stored on the basis of paragraph 1, but at the latest within 1 week of the lapsing of the retention periods under paragraph 1, such that this deletion cannot be reversed, or must ensure irreversible deletion.

§ 113c

Data usage

(1) The data stored on the basis of § 113b may

1. be transmitted to a criminal prosecution authority if this authority demands transmission by invoking a provision of the law which allows it to collect the data referred to in § 113b for the purpose of prosecuting particularly serious criminal offences;

2. be transmitted to a public risk prevention authority in the Federal States if this authority demands transmission by invoking a provision of the law which allows it to collect the data referred to in § 113b for the purpose of averting specific risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings;

3. be used by the provider of publicly available telecommunications services for information purposes according to § 113(1) sentence 3.

(2) The data stored on the basis of § 113b by the parties obligated in accordance with § 113a(1) may not be used for purposes other than those stated in paragraph 1.

(3) The data are transmitted in accordance with the statutory instrument pursuant to § 110(2) and the Technical Guideline as per § 110(3). The data must be identified in such a way that it can be discerned that it constitutes data which was stored in accordance with § 113b. Once the data has been transmitted to another authority, the latter must maintain this identification.

§ 113d

Ensuring data security

The party obligated in accordance with § 113a(1) must ensure that the data stored on the basis of the storage obligation under § 113b(1) is protected against unauthorised disclosure and use by means of state-of-the-art technical and organisational measures. The measures include, in particular,

1. the use of a particularly secure cipher,

2. storage in separate storage devices which are distinct from those used for standard operational tasks,

3. storage with a high level of protection against internet-based access on data processing systems which are uncoupled from the internet,

4. limiting access to the data processing equipment to persons who are specifically authorised by the obligated party and

5. the necessary cooperation of at least 2 persons when accessing the data who have been specifically authorised to this end by the obligated party.

§ 113e

Logging

(1) The party obligated in accordance with § 113a(1) must ensure that every instance of access to the data stored on the basis of the storage obligation under § 113b(1), in particular reading, copying, modification, erasure and blocking, is logged for data protection control purposes. The following must be logged:

1. the time of access,

2. those persons accessing the data,

3. the purpose and nature of the access.

(2) The protocol control information may not be used for purposes other than data protection control.

(3) The party obligated in accordance with § 113a(1) must ensure that the protocol control information is deleted after 1 year.

§ 113f

Catalogue of requirements

(1) When implementing the obligations pursuant to §§ 113b to 113e, a particularly high standard of data security and data quality must be guaranteed. Compliance with this standard is assumed if all the requirements laid down in the catalogue of technical arrangements and other measures drawn up by the Federal Network Agency, in consultation with the Federal Office for Information Technology Security and the Federal Data Protection and Freedom of Information Commissioner, are satisfied.

(2) The Federal Network Agency shall review on an ongoing basis the requirements contained in the catalogue in accordance with paragraph 1 sentence 2. In so doing, it will take into account the state-of-the-art and expert discussions. If the Federal Network Agency determines a need for change, the catalogue must be adapted immediately in consultation with the Federal Office for Information Technology Security and the Federal Data Protection and Freedom of Information Commissioner.

(3) § 109(6) sentences 2 and 3 shall apply accordingly. § 109(7) shall apply with the proviso that the requirements under paragraph 1 sentence 1, § 113b(7) and (8), § 113d and § 113e(1) and (3) shall supersede the requirements under § 109(1) to (3).

§ 113g

Security concept

The party obligated in accordance with § 113a(1) shall also incorporate the following in the security concept as per § 109(4):

1. the systems which are operated for the purpose of fulfilling the obligations arising from §§ 113b to 113e,

2. the hazards which shall be assumed for these systems and

3. the technical arrangements or other measures which have been taken or planned in order to counter these hazards and satisfy the obligations arising from §§ 113b to 113e.

The party obligated in accordance with § 113a(1) must present the security concept to the Federal Network Agency immediately after storage starts in accordance with § 113b and also immediately in the event of any modification to the concept. If the security concept does not change, the party obligated in accordance with § 113a(1) must explain this to the Federal Network Agency at intervals of 2 years each time."

3. The following sentence is added to § 121(1):

"In the report, the Federal Network Agency shall also communicate

1. the extent to which, and with what results, it has reviewed the security concepts as per § 113g and compliance therewith and

2. whether and which complaints and further outcomes the Federal Data Protection and Freedom of Information Commissioner has communicated to the Federal Network Agency (§ 115(4) sentence 2)."

4. § 149 is amended as follows:

a) Paragraph 1 is amended as follows:

aa) In point 35, the word "or" is replaced by a comma.

bb) The following points 36 to 44 are inserted after point 35:

"36. contrary to § 113b(1), also in conjunction with § 113b(7), does not store data, or does not do so correctly, in full, in the prescribed manner, for the specified duration or in good time,

37. fails to ensure, contrary to § 113b(1), in conjunction with § 113a(1) sentence 2, that the data mentioned therein is stored, or fails to communicate this fact, or does not do so correctly, in full or in good time,

38. contrary to § 113b(8), does not delete data, or does not do so in good time, or fails to ensure that the data are deleted in good time,

39. contrary to § 113c(2), uses data for purposes other than those mentioned,

40. fails to ensure, contrary to § 113d sentence 1, that data are protected against unauthorised disclosure and use,

41. fails to ensure, contrary to § 113e(1), that every instance of access is logged,

42. contrary to § 113e(2), uses protocol control information for purposes other than those mentioned,

43. fails to ensure, contrary to § 113e(3), that protocol control information is deleted in good time,

44. contrary to § 113g sentence 2, fails to present the security concept or does not do so in good time or".

cc) The previous point 36 becomes point 45.

b) Paragraph 2 sentence 1 is worded as follows:

"The administrative offence is punishable as follows:

1. In the cases referred to in paragraph 1 point 4a, points 6, 10, 22, 27, 31 and 36 to 40, with a fine of up to EUR 500 000,

2. in the cases referred to in paragraph 1 point 7a, points 16 to 17a, 18, 26, 29, 30a, 33 and 41 to 43, with a fine of up to EUR 300 000,

3. in the cases referred to in paragraph 1 point 4b, points 7b to 7d, 7g, 7h, 12 to 13b, 13d to 13o, 15, 17c, 19 to 21, 21b, 30 and 44, as well as paragraph 1a points 1 to 5, with a fine of up to EUR 100 000,

4. in the cases referred to in paragraph 1 points 7, 8, 9, 11, 17b, 21a, 21c, 23 and 24, with a fine of up to EUR 50 000, and

5. in the other cases referred to in paragraph 1, as well as in the case referred to in paragraph 1a point 6, with a fine of up to EUR 10 000."

5. The following paragraph 13 is added to § 150:

"(13) The retention obligation and the associated obligations under §§ 113b to 113e and 113g must be satisfied at the latest as of … [insert: date of the first day of the 19th calendar month following the promulgation of this Act]. The Federal Network Agency shall publish the catalogue of requirements to be drawn up in accordance with § 113f(1) sentence 2 at the latest on … [insert: date of the first day of the 13th calendar month following the promulgation of this Act].

Article 3

Amendment of the Act implementing the Code of Criminal Procedure

The following § 12 is added to the Act implementing the Code of Criminal Procedure in the revised version published in Federal Law Gazette III, volume number 312-1, as last amended by ...:

"§ 12

Transitional provision relating to the Act introducing a storage obligation and a maximum retention period for traffic data

(1) Location data stored in accordance with § 96(1) sentence 1 point 1 of the Telecommunications Act may be collected until … [insert: date of the day 4 weeks hence from the day designated in § 150(13) sentence 1 of the Telecommunications Act] on the basis of § 100g(1) of the Code of Criminal Procedure in the version applicable until the entry into force of the Act introducing a storage obligation and a maximum retention period for traffic data of … [insert: the date of issue and publication reference].

(2) The synopsis as per § 101b of the Code of Criminal Procedure, as amended by Article 1 of the Act of … [insert: the date of issue and publication reference of this Act] must be drawn up for the first time in relation to the year under review … insert: the number of the year following the date of the first day of the 19th calendar month following the promulgation of this Act]. § 100g(4) of the Code of Criminal Procedure in the version applicable until the entry into force of the Act introducing a storage obligation and a maximum retention period for traffic data shall be applied to the preceding years under review."

Article 4

Amendment of the Court Allowances Act

The Court Allowances Act of 5 May 2004 (Federal Law Gazette I pp. 718, 776), as last amended by …, is amended as follows:

1. The following statement is added to the Table of contents:

   "Appendix 3 (re § 23(1))".

2. In § 6(1), the words "§ 4(5) sentence 1, point 5 sentence 2 of the Income Tax Act determines" are replaced by the words "of the subsistence allowance for compensating additional job-related expenditure that has actually been incurred in Germany is calculated in accordance with the Income Tax Act ".

3. In § 23(2) sentence 1, in the part of the sentence before point 1, and under point 1 itself, every occurrence of the words "criminal prosecution authority" are replaced by the words "criminal prosecution authority or prosecuting agency".

4. The following heading is inserted after the heading to Appendix 2, Section 1:

"Preliminary observation 1:".

5. Appendix 3 is amended as follows:

a) In paragraph 2 of the General preliminary observation, the words "300 to 312, 400 and 401" are replaced by the words "300 to 321 and 400 to 402".

b) The following point 202 is inserted after point 201:

No.	Activity	Amount
"202	It is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 201 is	EUR 40.00".

c) Section 3 is worded as follows:

No.	Activity	Amount
	"Section 3 ***Information concerning traffic data***	
300	Information concerning stored traffic data: for every identifier underlying the exchange of information ..... Notification of the location data relating to the identifier is remunerated.	EUR 30.00
301	For the information, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 300 is	EUR 35.00
302	In the case of number 300, the information is provided on the basis of a uniform request also or solely in relation to traffic data which accumulates in future at specific times: for the second and every subsequent part of the information required in the request.....	EUR 10.00
303	Information concerning stored traffic data relating to calls made to a specific destination address by searching through all the records of the outgoing calls made by an operator (speed dialling search): for each destination address ..... Notification of the destination address location data are remunerated.	EUR 90.00
304	For the information, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 303 is	EUR 110.00
305	In the case of number 303, the information is provided on the basis of a uniform request also or solely in relation to traffic data which accumulates in future at specific times: for the second and every subsequent part of the information required in the request	EUR 70.00
306	Information concerning stored traffic data relating to a radio cell designated by the criminal prosecution authority (radio cell inquiry)	EUR 30.00
307	For the information, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 306 is	EUR 35.00
308	Information concerning stored traffic data relating to more than one radio cell designated by the criminal prosecution authority: Flat rate number 306 increases for every subsequent radio cell by	EUR 4.00
309	Information concerning stored traffic data relating to more than one radio cell designated by the criminal prosecution authority and, for the information, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 306 increases for every subsequent radio cell by	EUR 5.00

No.	Activity	Amount
310	Information concerning stored traffic data in instances where only the location and time are known: The inquiry is undertaken in relation to a specific location designated by an address	EUR 60.00
311	For the information, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 310 is	EUR 70.00
	The information relates to an area:	
312	- The distance between the points furthest removed from one another is not more than 10 km: Flat rate number 310 is	EUR 190.00
313	- The distance between the points furthest removed from one another is more than 10 but does not exceed 25 km: Flat rate number 310 is	EUR 490.00
314	- The distance between the points furthest removed from one another is more than 25 but does not exceed 45 km: Flat rate number 310 is ..... If the points furthest removed from one another are more than 45 km apart, the compensation in accordance with numbers 312 to 314 shall be calculated separately for the distance over and above this.	EUR 930.00
	The information relates to an area and it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act:	
315	- The distance between the points furthest removed from one another is not more than 10 km: Flat rate number 310 is	EUR 230.00
316	- The distance between the points furthest removed from one another is more than 10 but does not exceed 25 km: Flat rate number 310 is	EUR 590.00
317	- The distance between the points furthest removed from one another is more than 25 but does not exceed 45 km: Flat rate number 310 is ..... If the points furthest removed from one another are more than 45 km apart, the compensation in accordance with numbers 315 to 317 shall be calculated separately for the distance over and above this.	EUR 1 120.00
318	The information relates to a specific distance: For every 10 km of distance, or part thereof, flat rate number 310 is	EUR 110.00
319	The information relates to a specific distance and it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: For every 10 km of distance, or part thereof, flat rate number 310 is	EUR 130.00
320	Implementation of an order for transmitting traffic data which accumulates in future in real time: per connection ..... The compensation also remunerates the expenditure associated with disconnecting the transmission and notification of the location data relating to the connection.	EUR 100.00
321	Extension of the measure in the case of number 320	EUR 35.00
	Line costs for transmitting traffic data in the case of numbers 320 and 321:	
322	- if the transmission ordered does not last longer than 1 week	EUR 8.00
323	- if the transmission ordered lasts longer than 1 week but no longer than 2 weeks	EUR 14.00
324	- if the transmission ordered lasts longer than 2 weeks for every month or part thereof	EUR 25.00
325	Transmitting the traffic data on a data medium	EUR 10.00

d) The following point 401 is inserted after point 400:

No.	Activity	Amount
"401	In the case of number 400, it is necessary to use traffic data in accordance with § 113b(2) to (4) of the Telecommunications Act: Flat rate number 400 is	EUR 110.00

e) The previous point 401 becomes point 402.

Article 5

Amending the German Criminal Code

The German Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I p. 3322), as last amended by ..., is amended as follows:

1. In the Table of contents, the following entry is inserted after the information under § 202c:

"§ 202d Receiving stolen data".

2. The following § 202d is inserted after § 202c:

"§ 202d

Receiving stolen data

(1) Any party which makes available for himself, or to someone else, data (§ 202a(2)) which is not publicly available and which another party has acquired as a result of an unlawful act, which relinquishes said data to another party, or disseminates the data or makes it available in another way, in order to make money for himself or a third party or to injure someone else, shall face a prison sentence of up to 3 years or incur a fine.

(2) The punishment may not be more severe than that threatened in relation to the prior offence.

(3) Paragraph 1 shall not apply to actions which assist exclusively in fulfilling lawful, official or professional obligations. These particularly include

1. those activities of officials or their representatives by means of which data are to be supplied exclusively for utilisation in a taxation procedure, criminal proceedings or non-compliance procedures and

2. those professional activities of the persons mentioned in § 53(1) sentence 1 point 5 of the Code of Criminal Procedure by means of which data are received, evaluated or published."

3. § 205 is amended as follows:

a) In paragraph 1 sentence 2, the statement "and 202b" is replaced by a comma and the statement "202b and 202d".

b) In paragraph 2 sentence 1, the statement "§§ 202a and 202b" is replaced by the statement "§§ 202a, 202b and 202d".

Article 6

Restriction of a fundamental right

Articles 1 and 2 of this Act restrict telecommunications secrecy (Article 10 of the Basic Law).

Article 7

Entry into force

This Act shall enter into force on the day following promulgation.

Explanatory statement

A. General Part

I. Reason and objective of the draft Act

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105 of 13 April 2006, p. 54; hereinafter referred to as the Data Retention Directive) made provision for the introduction of an obligation to store such data. It was transposed into German law by means of the Act re-regulating telecommunications monitoring and other covert investigative measures and transposing Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette I p. 3198). In §§ 113a and b of the Telecommunications Act, it made provision for an obligation on the part of service providers to store traffic data of their subscribers for 6 months and to make this data available to the criminal prosecution authorities on request. In accordance with the new regulation under § 100g of the Code of Criminal Procedure, *inter alia*, the criminal prosecution authorities were authorised to retrieve the data where it is suspected that a criminal offence has been committed which is also of considerable importance in a given case.

In its judgment of 2 March 2010 (1 BvR 256/08; Federal Constitutional Court Decisions 125, 260), the Federal Constitutional Court declared §§ 113a and 113b of the Telecommunications Act, and also § 100g(1) sentence 1 of the Code of Criminal Procedure, insofar as traffic data as per § 113a of the Telecommunications Act could be collected in accordance with these provisions, to be invalid on account of an infringement of Article 10(1) of the Basic Law. In its judgment of 8 April 2014, the Court of Justice of the European Union declared the Data Retention Directive underlying the Implementation Act to be void on account of an infringement of Articles 7 and 8 of the Charter of Fundamental Rights. An obligation therefore no longer exists under European law regarding the legal introduction of an obligation for the providers of publicly available telecommunications services to store traffic data for a certain period of time.

The current legal situation, however, leads to shortcomings in connection with crime prevention and protecting against threats. Indeed, the criminal prosecution authorities are able to access traffic data which is still stored by the providers of publicly available telecommunications services on commercial grounds at the time of the inquiry on the basis of § 100g(1) of the Code of Criminal Procedure where there are initial grounds for suspicion and a corresponding judicial order exists. The providers of publicly available telecommunications services may store traffic data designated in detail in the Telecommunications Act in particular also upon completion of the specific communications process if they require this data for their own – specifically stipulated in the Telecommunications Act – needs (e.g. establishing further connections, billing, trouble-shooting or protecting against nuisance calls, § 96 of the Telecommunications Act). Since the storage practices adopted by providers of publicly available telecommunications services vary widely, it therefore comes down to chance at present as to which data can be retrieved in the case of an inquiry as per § 100g of the Code of Criminal Procedure.

A change in this state of affairs is also indicated with respect to the importance of an effective prosecution. The Federal Constitutional Court has repeatedly highlighted the requirement under constitutional law for effective prosecution, emphasised the interest in ascertaining the truth in criminal proceedings as fully as possible, and labelled the effective investigation of especially serious criminal offences as an important mandate of a

constitutional community (Federal Constitutional Court Decisions 129, 208 <260> with further references). The European Court of Human Rights inferred from Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms positive obligations on the part of States in terms of applying substantive criminal law in practice by means of effective investigation and prosecution (ECHR, No. 2872/02, 2 December 2008 – K.U. v. Finland). The Court of Justice of the European Union also emphasised the importance of combating serious crime in order to guarantee public security (CJEU judgment on Digital Rights, C-293/12 and C-564/12, EuZW [European Journal of Economic Law] 2014, 459 <462>, recital 42).

The draft Act remedies the shortcomings described in connection with crime prevention and protecting against threats. As a result of storing the traffic data for a limited period, additional opportunities in terms of investigation are created which take account of the increasing importance of telecommunications when it comes to preparing and committing crimes. At the same time, the draft Act satisfies the requirements laid down in Article 10(1) of the Basic Law as specified by the Federal Constitutional Court in the aforementioned judgment. Data stored unconditionally by way of precaution is subject to particularly stringent requirements, both in terms of its justification and also its configuration, in particular also with respect to its intended purposes (Federal Constitutional Court Decisions 125, 260 <316 f.>).

On the one hand, these standards concern data security. The Federal Constitutional Court has remarked that the security of the data must be guaranteed both during retention and also during transmission. Moreover, effective safeguards designed to ensure that the data are deleted are required. The constitution does not specify in detail which security stipulations are required in particular. A high standard which is guided by the state of the art must be retained, however, and new findings and insights incorporated on an ongoing basis. It is obvious that in principle, separate data retention, sophisticated encoding, a secure access regime taking account, for instance, of the "principle that two pairs of eyes are better than one" and audit-proof logging ought to be guaranteed. The legislator is able to entrust a supervisory body with the technical expression of the security standards to be specified under law. The legislator must ensure that the decision regarding the nature and extent of the protective measures to be taken does not ultimately lie unchecked in the hands of the providers. Under constitutional law, a publicly transparent check involving the independent Data Protection Commissioner and a balanced system of sanctions which also ascribes appropriate importance to data security infringements is required.

Data usage must also be proportionate. For prosecution purposes, data may only be retrieved in the event that certain facts give cause for justified suspicion that a serious crime has been committed which also has to be taken seriously in a given case. The criminal offences which justify retrieval must be definitively laid down by the legislator in the form of a catalogue. Moreover, it must be ensured under law that the data are evaluated as soon as it is transmitted and deleted if it is irrelevant to the purposes of collection. The data may only be passed on to other authorities if effected with a view to carrying out tasks on account of which access would also be permitted directly. In order to ensure this, the data stored unconditionally by way of precaution must be identified in a particular way. The legislator has room to manoeuvre as regards the scope of the data to be retrieved. Under constitutional law, however, it is necessary to make provision for a fundamental ban on transmission at least in relation to a tightly-knit circle of telecommunication links which rely on exceptional confidentiality. Consideration must be given in this regard, for example, to calls made to lines of persons, public authorities and organisations working for the church or in the social domain, who or which offer counselling wholly or predominantly by telephone to callers in emotional or social distress who remain essentially anonymous and where these individuals themselves, or the employees of these authorities and organisations, are subject to other non-disclosure obligations in this respect (cf. § 99(2) of the Telecommunications Act).

Finally, the legislator must take adequate precautionary measures regarding transparency of data use. Where possible, the data must be used in an open manner. Otherwise, it shall at least require in principle that the persons concerned are notified subsequently. If, exceptionally, this does not happen either, the non-notification shall require a court order. Effective legal protection presupposes that data retrieval is at the discretion of a judge and that there is a redress mechanism for ex-post monitoring of how the data are used. Effective sanctions in the case of violations of rights are a further necessary element of a proportional provision.

In addition to the stipulations under the Basic Law, however, the stipulations under the Charter of Fundamental Rights, as specified by the Court of Justice of the European Union in its judgment of 8 April 2014 concerning Directive 2006/24/EC, must be taken into account. According to Article 51(1) of the Charter of Fundamental Rights, Member States are bound by this Charter when implementing Union law. That is the case if a national regulation falls within the scope of EU law. The fundamental applicability of the Charter of Fundamental Rights to national regulations concerning the retention of data results from Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications): After the Court of Justice of the European Union declared Directive 2006/24/EC to be invalid, the area of application under Article 15(1) of Directive 2002/58/EC is reopened in relation to national regulations concerned with the storage of telecommunications data. According to this article, national regulations concerning the retention of data are permitted in relation to the prevention, investigation, detection and prosecution of criminal offences provided they satisfy the requirements laid down in Article 6(1) and (2) of the Treaty on European Union. Thus, the binding of possible national regulations to the Charter follows from Article 15(1). In addition, the applicability of Article 15 ensures that national regulations come under the scope of EU law.

The judgment of the Court of Justice of the European Union demonstrates why the retention of data, as provided for in Directive 2006/24/EC, is incompatible with the Charter of Fundamental Rights. The Court of Justice is critical of the fact that the Directive affects all individuals, electronic means of communication and traffic data across the board without making any distinction or restriction on the basis of the aim of prosecuting serious criminal offences. For example, the Directive also applies to individuals whose communication processes are covered by professional secrecy in accordance with national legislation. Furthermore, the Directive does not contain any objective criterion allowing access by national authorities to the data and the utilisation thereof to be limited to those serious cases which justify an intervention but leaves this to the Member States. The Directive does not make provision for any mechanism for prior monitoring by courts or independent administrative bodies of access to the stored data by the national authorities. The Directive also makes provision for a retention period of at least 6 months without making a distinction on the basis of the category of data in accordance with its possible use in relation to the objective pursued or on the basis of the persons affected. Objective criteria which ensure that the retention period of between 6 and 24 months is restricted to what is absolutely necessary are lacking. Moreover, the directives do not offer sufficient guarantees in terms of safeguarding the stored data adequately against the risks of abuse. Instead, it allows the providers of publicly available telecommunications services to take economic criteria into consideration when determining the security level applied. Finally, the Court of Justice rebukes the fact that the Directive does not prescribe any data storage within the European Union's territory, meaning that compliance with the data protection requirements under EU law cannot be fully guaranteed.

If the view is taken in part that the Court of Justice of the European Union regards traffic data stored unconditionally per se as being incompatible with the Charter of Fundamental Rights, this cannot be upheld. Directive 2006/24/EC underlying the review undertaken by the Court of Justice of the European Union has a variety of points of criticism which, when

considered as a whole, have justified the disproportionate nature of the data retention under Directive 2006/24/EC. Above all, the combination of comprehensive data storage for a period of between 6 and 24 months without the possibility of differentiating between types of data or the purpose of storage shall result, according to the judgment of the Court of Justice, in a disproportionate provision in Directive 2006/24/EC. Furthermore, account needs to be taken of the fact that the Data Retention Directive only contains provisions relating to the storage of traffic data. The regulation of the preconditions concerning retrieval was reserved for the Member States in the absence of a competence basis under EU law (Article 4 of the Directive). In fact, the Directive thus made provision for the collection of personal data to be retained for purposes which are still to be determined. The Federal Constitutional Court also deems data collection such as this to be illegal (Federal Constitutional Court Decisions 125, 260 <320 f.>). The decision concludes that retention may be proportionate, however, and hence permissible if undertaken for specific purposes and embedded in a statutory framework which is appropriate for intervention. The proportional elaboration of the provisions concerning data usage already has a retroactive effect upon the constitutionality of the retention as such. Against this background, the judgment of the Court of Justice of the European Union is understood to mean that when differentiating between the data to be retained and, at the same time, in the case of a reduction in the data set, the specific and restrictive designation of the retention and intended purposes, the considerable reduction in the retention period and the creation of additional material and technical preconditions, the storage of telecommunications data in connection with crime prevention and for protecting against threats can be shaped in a manner which is in keeping with fundamental Union law.

The draft Act satisfies the stipulations referred to under constitutional and European law by combining a storage obligation which is as short as possible with stringent retrieval regulations. It makes provision, on the one hand, for a ten-week retention of precisely designated traffic data (in the case of location data, even just a four-week retention period) by the providers of publicly available telecommunications services for the purposes of crime prevention and for protecting against threats and, on the other, facilitates the retrieval of data by government agencies only under very strict conditions.

In keeping with the requirements of the Court of Justice of the European Union, the retention obligation is already limited to what is strictly necessary. Data from electronic mail services are entirely exempt from the storage obligation. To protect the particular relationship of trust, traffic data which relates to persons, public authorities and organisations working for the church or in the social domain, who or which offer counselling wholly or predominantly by telephone to callers in emotional or social distress who remain essentially anonymous and where these individuals themselves, or the employees of these authorities and organisations, are subject to particular non-disclosure obligations in this respect, is essentially exempt from the storage obligation. Detailed regulations which provide legal clarity limit data usage and ensure its security.

Collection of the traffic data stored on a compulsory basis is also strictly limited. This data may only be retrieved for the purpose of prosecuting particularly serious criminal offences indicated under § 100g(2) of the Draft Code of Criminal Procedure which also have to be taken particularly seriously in a given case. With respect to the high level of relevance in terms of fundamental rights of the retrieval of data stored on a compulsory basis, the catalogue in accordance with § 100g(2) of the Draft Code of Criminal Procedure is significantly reduced compared with that under the preceding regulation (criminal offences of major importance). In this way, account is taken of the fact that the Court of Justice of the European Union only deemed the storage of traffic data to be permissible if the combating of serious crime is at issue. The catalogue includes criminal offences which assist in the combating of terrorism or the protection of personal objects of legal protection, in particular the protection of life and limb, freedom and sexual self-determination. Particularly serious crimes where the stored traffic data can prove to be particularly valuable, based on criminological experience, are also covered.

It is also stipulated that the criminal prosecution authorities may not collect traffic data in connection with all people authorised to refuse testimony in accordance with § 53 of the Code of Criminal Procedure. Accidental discoveries shall be banned from being exploited. As regards the retrieval of data, provision is made for comprehensive discretion on the part of judges; the public prosecutor's office is not able to act in urgent matters. Moreover, data collection is organised as an overt measure. In principle, the persons concerned must be notified prior to the data being retrieved. Notification may be deferred by way of exception. This does require a court order, however.

For the purposes of protecting against threats, the collection of data are likewise only possible under strict conditions. Retrieval must assist in averting the most serious risks, i.e. risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings.

The collection of particularly sensitive location data are severely limited compared with current law. Unlike previously, in order to establish whereabouts, reference may not be made to traffic data stored for commercial purposes. Location data may only be collected under the strict conditions laid down in paragraph 2.

The draft Act also defines in more precise terms the preconditions concerning radio cell inquiries regulated hitherto in § 100g(2) sentence 2 of the Code of Criminal Procedure. As a result of radio cell inquiries, traffic data pertaining to third parties, i.e. those persons who, without being a suspect or conveyor of (illegal) communications, have communicated using their mobile telephone in the radio cell being inquired about, is unavoidably collected on a regular basis. Traffic data pertaining to non-participants may not be collected over and above the extent which is strictly necessary in order to prosecute. To this end, the radio cell inquiry is given a legal definition and the rigorous subsidiarity clause under § 100a(1) point 3 of the Code of Criminal Procedure adopted. In addition, as before, the radio cell inquiry must declare the telecommunication to be acquired as being geographically limited, short-term and sufficiently specific. In this way, the compilation of movement profiles of respectable citizens is effectively prevented.

The protection under criminal law of information systems and the data stored in them against attacks and illicit access is tantamount to the matter of facilitating effective prosecution in a society increasingly characterised by information and communication technology. This protection must also be directed against acts constituting the offence by means of which tracked or intercepted data, or data unlawfully acquired in another way, is handled and so that the encroachment on the formal right of disposal of their data on the part of the authorised individual, which is effected by means of the prior offence, is continued and intensified.

Data espionage and phishing and preparatory work relating to these deeds are already made a punishable offence today in accordance with §§ 202a, 202b and 202c of the German Criminal Code which transpose the corresponding stipulations of the Convention of the Council of Europe on Cybercrime of 23 November 2001, which has been ratified by the Federal Republic of Germany, of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (OJ L 69 of 16 March 2005, p. 67) and of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218 of 14 August 2013, p. 8). Regarding the transposition in full of the Directive on attacks against information systems, furthermore, an increase in the range of sentences under § 202c of the German Criminal Code (Acts preparatory to data espionage and phishing) is necessary. This is to happen by means of the Anti-Corruption Act (*Bundestag* document no. 18/4350) presented by the Federal German Government.

Also, the trade in data which has been obtained as a result of data espionage and phishing or by means of other unlawful acts can already be subject to certain statutory

offences. The currently applicable provisions under criminal law are inadequate, however, and have loopholes in terms of protection which are to be closed by means of a separate criminal offence of receiving stolen data.

Under existing law, as regards the purchase and sale of stolen data, liability to punishment in accordance with § 202c(1) point 1 of the German Criminal Code (Acts preparatory to data espionage and phishing) comes into consideration in particular. Accordingly, any party which makes available for itself, or to someone else, passwords or other security codes which facilitate access to data, or which sells or relinquishes these to another party, or disseminates or makes them available in another way, shall be guilty of an offence if, as a result, the party is committing acts preparatory to data espionage and phishing (§§ 202a, 202b of the German Criminal Code). Liability to punishment also therefore covers the trade in certain data which has been acquired as a result of acts which are liable to prosecution. It is, however, limited to passwords and other security codes which facilitate access to data and thereby do not cover in any event, for example, the trade in account-related and credit card data if this data are to be used directly for payment purposes without the perpetrator being provided in the process with access to data which is not intended for them and which is specially protected against unauthorised access (Golla/von zur Mühlen, *Juristenzeitung* – JZ 2014, pp. 668, 672). Even where passwords and security codes are available, liability to punishment in accordance with the provision is excluded if the perpetrator acquires the data for resale and does not have any sufficiently concrete intention regarding the preparations to commit an offence in accordance with §§ 202a and 202b of the German Criminal Code (cf. *Leipziger Kommentar*/Hilgendorf, 12th edition, § 202c, recital 26 *et seq.*).

Also, involvement on the part of the perpetrator who received stolen data in the preceding criminal offences of data espionage or phishing in accordance with §§ 202a and 202b of the German Criminal Code is ruled out if these crimes have already been concluded, which will regularly be the case, at the time the data are acquired. Nor does involvement in a possible subsequent culpable use of the data, such as computer fraud (§ 263a of the German Criminal Code) and forgery of data intended to provide proof (§ 269 of the German Criminal Code) come into consideration as long as the perpetrator only acquires and resells the data without it being used subsequently in a culpable manner by the (wholesale) buyer or in the absence of this being established.

According to the Federal Data Protection Act [German designation: BDSG], the collection, processing, retrieval and making available for oneself, or to someone else, of unauthorised personal data which is not publicly available shall be liable to prosecution if the act is committed in return for money or with the intention of making money for themselves, or a third party, or injuring someone else (§ 44 in conjunction with § 43(2) points 1 and 3 of the Federal Data Protection Act). Liability to punishment shall exist irrespective of whether the data has been acquired beforehand as a result of an unlawful act. It cannot therefore also include the specific unlawful content of the trade in data which has been acquired by a prior perpetrator as a result of espionage or phishing or which has been otherwise obtained as a result of an unlawful act. As regards receiving stolen data, the perpetrator takes advantage of the infringement which was punishable as a result of the prior offence and therefore acts in a more reprehensible manner than is the case when merely handling personal data when not authorised to do so as is covered by the Federal Data Protection Act. The unlawful content, which is of a different nature and which falls short of the criminal offences under the Federal Data Protection Act, is reflected in particular in a modest threat of punishment (up to 2 years' imprisonment) and in the elaboration of the standard as an unmitigated offence requiring an application for prosecution, in which connection, in addition to the person concerned under data protection law, the responsible authority and the supervisory data protection authorities are authorised to file the application. Neither satisfy the unlawful content of receiving stolen data. Particularly in the case of massive attacks on information systems involving a large number of injured parties but who, individually speaking, are only marginally affected

as regards their objects of legal protection, and where it is therefore conceivable that they shall refrain from submitting an application regarding demand for prosecution as is required under the Federal Data Protection Act, the trade on a massive scale in data obtained as a result of espionage following the attack cannot be adequately prosecuted and punished under criminal law. The provisions of the Federal Data Protection Act shall also only apply to personal data, i.e. to particulars concerning personal and material circumstances of an identified or identifiable natural person (§ 3(1) of the Federal Data Protection Act), and do not cover, for example, the trade in data of legal entities. As regards the trade in non-personal data, liability to punishment on account of the breach of business and trade secrets in accordance with the provision under § 17 of the Protection against Unfair Competition Act [German designation: UWG] does indeed come into consideration. In keeping with its protective purpose, however, the standard shall likewise not apply in a wholesale manner.

In accordance with § 17(2) point 2 of the Protection against Unfair Competition Act, a party shall be liable to prosecution when it exploits in an unauthorised manner a business or trade secret which it has obtained or secured without the requisite authority or if it communicates it to someone else. Business and trade secrets shall be deemed to exist only if the secret relates to the business operation, the data in question is not commonly known, and the business owner has a desire and interest in keeping this data secret. For example, there may be an absence of credit card-related data which is used in the context of daily business dealings. The purchase and sale of such data which has been acquired beforehand as a result of espionage or by means of another unlawful act is not punishable in these instances in accordance with § 17 of the Protection against Unfair Competition Act.

Given the existing gaps in criminal liability, in 2012, the 69th session of *Deutscher Juristentag* [Association of German Jurists] also argued in favour of the introduction of making "receiving stolen data" a criminal offence. A corresponding draft Act was tabled by the *Bundesrat* in the Lower House of the German Parliament (*Bundestag* document no. 18/1288). The existing draft regulation is based on this draft Act.

Data, particularly data relating to criminal offences where perpetrators penetrate foreign computer systems and gain access to data (hacking, § 202a of the German Criminal Code), or where data are intercepted when it is transmitted (§ 202b of the German Criminal Code), is available as stolen goods. In the process, the prior perpetrators circumvent password protection using technical means, for example or exploit security loopholes in order to install undetected malware. By means of such attacks against information systems, they can, for instance, acquire enormous quantities of stored data from providers of telecommunications services, social networks or email services, as well as from banks, which is then used to commit further criminal offences, not necessarily by the perpetrators themselves, but rather is offered for sale to third parties. Data may also be obtained by deceiving the authorised individual, something which is liable to prosecution on the basis of § 269 of the German Criminal Code (Forgery of data intended to provide proof), for instance, by means of so-called phishing, where the user transmits confidential access data, including user name, passwords, PIN and TAN numbers, to a supposedly trustworthy contact who has assumed a false identity, generally by email (Sieber, opinion C to the 69th session of *Deutscher Juristentag*, 2012, p. 20). Data acquired in this way is also traded by international groups structured according to the division of labour who use special – largely not accessible by the general public – discussion fora and chat services to this end (Sieber, opinion C to the 69th session of *Deutscher Juristentag*, 2012, p. 22).

According to the police crime statistics of the Federal Criminal Police Office and the criminal justice statistics of the German Federal Statistical Office, following an earlier significant increase in recent years, an almost consistently high number of crimes against the integrity, confidentiality and availability of information technology systems shall be

assumed (see also Federal Criminal Police Office, Federal Situation Survey on Cybercrime 2013). These crimes constitute the black market in the stolen data trade.

The perpetrators are not necessarily pursuing just financial interests with the acquisition and disclosure of stolen data. Injuring third parties, for instance by means of attacks against information systems, may also be motive for the crime.

The new criminal offence of receiving stolen data safeguards formal data secrecy, which has already been infringed as a result of the prior offence, against the maintenance and consolidation of this infringement. The formal right of disposal on the part of that party which, on account of its right to intellectual content, shall take a decision on the disclosure and transmission of the data (*Münchener Kommentar*/Graf, 2nd edition, § 202a, recital 2) and, thereby, on its interest in maintaining the right of ownership over information (*Leipziger Kommentar*/Hilgendorf, 12th edition, § 202a, recital 6), is impaired as soon as the data are acquired by the prior perpetrator. With the prior offence, the decision which they are entitled to make as to the parties to whom their data are to be made available is taken out of the hands of the authorised individual.

This violation of an object of legal protection is maintained and intensified if, following this, a third party obtains the stolen data and this is then disseminated. When the stolen data are received, another individual shall have the opportunity to take a decision on making the data available instead of the authorised individual. At the same time, it may become more difficult for the authorised individual to keep track of their data and to reclaim sole right of disposal thereof.

In accordance with Federal Court of Justice case-law, the receipt of stolen property not only violates the property or assets already infringed as a result of the prior offence by maintaining and consolidating the unlawful condition of the assets brought about by the prior offence but also, above all, general security interests which have been impaired by the incentive to commit prior offences established by dealing in stolen goods (Federal Court of Justice, decision of 25 July 1996 – 4th constitutional law 202/96, Federal Court of Justice Statutes 7, 142, decision of 20 December 1954 – GSSt 1/5; cf. *Münchener Kommentar*, 2nd edition, § 259, recital 3). This shall apply, *mutatis mutandis*, to receiving stolen data. From this follows, on the one hand, restriction of the criminal offence of receiving stolen goods to unlawful prior offences, to the exclusion of other (non-punishable) illegal activities undertaken by the prior perpetrator. At the same time, this also explains the inclusion of such prior offences which, in a given case, are directed against the formal right of disposal on the part of the authorised individual, the liability to punishment of which, however (unlike the instances under §§ 202a and 202b of the German Criminal Code, for instance), is not based on a violation of the legally protected object of the formal right of disposal of data, but which serve to protect the other objects of legal protection.

Dealing in stolen data shall only be punishable, however, if the data in question is not available to the general public. Data can be duplicated as often as necessary and accessed by any number of individuals concurrently (Golla/von zur Mühlen, JZ 2014, pp. 668, 671). The authorised individual shall generally not be deprived in full of the data acquired by the prior perpetrator neither as a result of the prior offence nor the subsequent act of receiving stolen goods. Instead, this data shall continue to be available to them. Their formal right of disposal is not impaired in a punishable manner as a result of the purchase and sale of data stolen from them if the data in question can be taken from generally accessible sources and where the decision as to who the data are to be made available to shall therefore no longer rest solely in the hands of the authorised individual.

II. Key amendments

The draft Act essentially includes amendments to the Code of Criminal Procedure (Article 1), the Telecommunications Act (Article 2) and the German Criminal Code (Article 5).

1. Reorganisation of the collection of traffic data in accordance with § 100g of the Draft Code of Criminal Procedure

The stipulations of the Federal Constitutional Court and of the Court of Justice of the European Union in the decisions relating to the retention of data necessitate a fundamental reorganisation of § 100g of the Code of Criminal Procedure. On this occasion, the preconditions concerning radio cell inquiries are defined in more precise terms.

While the collection of traffic data which is stored by the providers of publicly available telecommunications services on commercial grounds is regulated in paragraph 1, paragraph 2 stipulates the preconditions under which the data retained henceforth as a result of the new storage obligation may be collected. The Federal Constitutional Court has expressly requested this differentiation (Federal Constitutional Court Decisions 125, 260 <328>):

"Use of the data pools acquired as a result of an unconditionally systematic storage of practically all telecommunications traffic data shall be subject accordingly to particularly stringent requirements. In particular, this is not permitted under constitutional law to the same extent as the use of telecommunications traffic data which the providers of publicly available telecommunications services may store in accordance with § 96 of the Telecommunications Act, depending on the respective operational and contractual conditions which can be influenced, in part, by the customers. In view of the unavoidability, integrity and, hence, increased significance of the traffic data systematically collected by way of precaution over a six-month period, its retrieval is disproportionately more important."

The collection of the traffic data stored in accordance with § 113b of the Draft Telecommunications Act should only be possible in accordance with § 100g(2) of the Draft Code of Criminal Procedure under very strict conditions, namely for the purpose of prosecuting particularly serious criminal offences specifically designated in § 100g(2) sentence 2 of the Draft Code of Criminal Procedure which also have to be taken particularly seriously in a given case. The catalogue in accordance with § 100g(2) of the Draft Code of Criminal Procedure is thereby significantly reduced compared with that under the preceding regulation.

The collection of stored location data are an especially sensitive matter because movement profiles can be compiled therefrom. It is therefore only authorised in accordance with paragraph 2 under the stringent preconditions regulated therein. Paragraph 1 essentially precludes the collection of location data stored on commercial grounds while establishing the whereabouts of the suspect is no longer among the permitted purposes of traffic data collection under this provision. The collection of location data which accumulates in future and location data in real time does not, however, draw on stored data and is permitted, as before, for investigating the facts of the case or establishing the whereabouts of the suspect under the preconditions laid down in paragraph 1 sentence 1 point 1.

When collecting traffic data, the key considerations regarding proportionality must be presented separately in the justification for its arrangement or extension (§ 101a(1) of the Draft Code of Criminal Procedure). This shall also apply to radio cell inquiries which are given a legal definition in the new paragraph 3.

2. Amendments to the Telecommunications Act

§ 113a specifies the circle of parties obligated to store traffic data and, for reasons of proportionality, includes a compensation scheme in the event that the storage obligation would lead to undue hardship.

§ 113b of the Draft Telecommunications Act prescribes the retention of precisely designated traffic data. In this regard, a distinction is drawn regarding the retention period. While the call detail records have to be stored for 10 weeks, the storage of particularly sensitive location data are limited to 4 weeks.

Otherwise, the requirements laid down in the Telecommunications Act essentially assist in transposing the stipulations of the Federal Constitutional Court and the Court of Justice of the European Union in their judgments relating to the retention of data and set out accordingly the specifics relating to the storage obligations, the use of the data and the guaranteeing of its security, as well as the logging of access thereto. Moreover, details are set out in relation to the catalogue of requirements concerning the technical arrangements and other protective measures to be drawn up by the Federal Network Agency and the security concept to be drawn up by the obligated enterprises.

3. Amendments to the German Criminal Code

The draft makes provision for the introduction of a new criminal offence of receiving stolen data (§ 202d of the Draft German Criminal Code). According to this, a party shall be liable to prosecution when it makes available for itself, or to someone else, data which is not publicly available which another party has acquired as a result of an unlawful act, when it relinquishes said data to another party, or when it disseminates the data or makes it available in another way, in order to make money for itself or a third party or to injure someone else. The act shall be threatened with a prison sentence of up to 3 years or a fine, in which connection the punishment may not be more severe than that threatened in relation to the prior offence.

The act shall only be prosecuted on request, unless the criminal prosecution authority officially deems intervention to be necessary on account of special public interest in the prosecution (§ 205(1) sentence 2 of the Draft German Criminal Code).

The provisions of the Code of Criminal Procedure, which relate to criminal offences after the fact, such as dealing in stolen goods in particular, are to be extended to the new criminal offence of receiving stolen data as consequential amendments.

III. Legislative powers

The legislative powers of the Federal Government follow from Article 74(1) point 1 of the Basic Law (judicial proceedings, criminal law) and Article 73(1) point 7 of the Basic Law (telecommunications). The introduction of §§ 113a to 113g in the Telecommunications Act does not involve provisions which would prompt a need for the Act to be approved in accordance with Article 87f(1) of the Basic Law. The provisions do not affect the "extensively appropriate and adequate service" within the meaning of Article 87f(1) of the Basic Law.

IV. Compatibility with European Union legislation and treaties under international law concluded by the Federal Republic of Germany

The draft Act is compatible with European law and treaties under international law concluded by the Federal Republic of Germany.

V. Legal consequences

1. Legal and administrative simplification

As a result of the provision in law of a storage obligation for traffic data, it shall be assumed that the collection of traffic data will be a success more frequently than is currently the case. This shall also apply to inventory data retrieval.

2. Sustainability aspects

The draft Act is in keeping with the basic ideas of the Federal [German] Government regarding sustainable development in the context of the national sustainability strategy. The intended provisions limit the restriction of citizens' protected interests under fundamental law to the bare minimum for safeguarding the concerns of criminal prosecution and, at the same time, take appropriate account of the key requirements of the criminal prosecution authorities. The draft Act also serves to improve the combating of offences associated with trade in data obtained illegally and, consequently, the combating of criminality (sustainability indicator 15). Given the considerable social and economic importance of data security, the unlawful trade in data acquired illegally is also countered using criminal law resources.

3. Budget expenditure without compliance costs

No budget expenditure without compliance costs shall accrue.

3. Compliance costs

a) Compliance costs for citizens

No additional compliance costs shall be incurred by citizens.

b) Compliance costs for businesses

Additional expense shall arise for the providers of publicly available telecommunications services in question each time as a result of fulfilment of the storage obligation provided for in § 113b of the Draft Telecommunications Act and the associated provisions concerning use of the data, the guaranteeing of data security and data quality, the logging of access to the data and the inclusion of certain information in the security concept to be drawn up. § 113a(2) of the Draft Telecommunications Act therefore includes a compensation scheme, for reasons of proportionality, which is primarily designed to protect small business owners from undue hardship.

The level of expenditure ought to vary in size, depending on the previous – very different and changing – ways in which the data are retained and the size of the undertaking. The necessary reorganisation shall, however, take place to some extent in the context of technical adaptations which are pending at regular intervals in any case and shall therefore be able to reduce the expenditure triggered solely as a result of the storage obligation.

The additional expenditure incurred in total by the telecommunications industry cannot be estimated at present. While the expenditure relating to traffic data collection and information retrieval as per § 23 of the Draft Court Allowances Act is compensated, the draft only makes provision for compensation vis-à-vis the investment and, where appropriate, increased operating costs required in order to fulfil the storage obligations if undue hardship would otherwise result.

Since the majority of the approximately 1 000 enterprises in question are small- to medium-sized providers of publicly available telecommunications services for which the anticipated costs of reorganisation will pose a considerable hardship, it is likely that many of them will claim compensation. It is assumed that the other enterprises in question will factor these costs into their pricing and pass them on to their customers.

The draft introduces the following new obligations to provide information within the meaning of the Act instituting a National Regulatory Council for enterprises and administration:

– § 113b(1) of the Draft Telecommunications Act obligates the providers of publicly available telecommunications services to retain data in accordance with paragraphs 2 and 3 for 10 weeks. In the case of location data as per paragraph 4, the storage obligation shall be 4 weeks.

– § 113e(1) of the Draft Telecommunications Act stipulates that the party obligated in accordance with § 113a of the Draft Telecommunications Act must log in an audit-proof manner any access to the stored data for data protection control purposes.

– § 113g sentence 1 of the Draft Telecommunications Act stipulates that the party obligated in accordance with § 113a of the aforementioned act must incorporate certain information in the security concept to be drawn up.

– § 113g sentence 2 of the Draft Telecommunications Act specifies the times at which the party obligated in accordance with § 113a of the aforementioned act must present the security concept to the Federal Network Agency. § 121(1) of the Draft Telecommunications Act extends the notification obligations of the Federal Network Agency in the progress report to be prepared.

As a result of the amendments to the Code of Criminal Procedure undertaken in this Act, it shall not entail any costs for businesses when their behaviour complies with standards. The Act is geared towards combating effectively the trade in data acquired illegally and can therefore contribute to businesses avoiding damages and thereby incurring costs.

c) Compliance costs for administration

§ 101b of the Draft Code of Criminal Procedure extends the obligations currently arising from § 100g(4) of the Code of Criminal Procedure relating to the collection of statistical data by the criminal prosecution authorities and the Federal Office of Justice. The resulting additional expenditure cannot yet be quantified at present.

As a result of the amendment of the provisions of the Telecommunications Act in Article 2, the Federal Network Agency shall incur additional enforcement costs, subdivided into real investment and personnel costs. The – on account of the stipulations of the Federal Constitutional Court in its judgment relating to the retention of data – unavoidable additional expense shall accrue, *inter alia*, as a result of the obligation pursuant to § 113f of the Draft Telecommunications Act to draw up a catalogue of requirements, review this on a continuous basis and adapt it immediately as required. Moreover, increased monitoring expenditure shall result from the obligation to store traffic data in the context of supervision under § 115 of the Telecommunications Act, including application of the new offences which could result in a fine. Additional costs shall also be incurred by the Federal Data Protection and Freedom of Information Commissioner within the framework of their control and supervisory activity as well as by the Federal Office for Information Technology Security in the context of its involvement in drawing up the catalogue of requirements pursuant to § 113f of the Draft Telecommunications Act.

The cost lump sums to be granted in accordance with the Court Allowances Act shall put a strain on the Federal State budgets. It is not anticipated, however, that this burden shall be substantially higher than is the case with the existing provisions.

The impact of the compensation scheme in § 113a(2) of the Draft Telecommunications Act is still to be assessed. Of the approximately 1 000 providers in existence, 20 are so big that they account for 98 % of the market, while the remainder are small- to medium-sized companies with only a few subscribers, in which connection it is anticipated that some will claim undue hardship regarding the investments to be made. This can only happen, however, if the corresponding catalogue of requirements (§ 113f of the Draft Telecommunications Act) has been drawn up by the Federal Network Agency.

A decision shall be taken in the context of future budgetary procedures regarding the financing of the budgetary burden associated with the draft legislation.

No impact on the budgets of the municipalities is anticipated.

4. Further costs

The traffic data inquiry does not constitute a new investigative tool. It is anticipated that the judiciary shall not incur any appreciable costs as a result of the amendments introduced by means of this Act since the level of inquiries on the part of the criminal prosecution authorities ought to, by and large, be the same as before but will lead to better outcomes. In these instances, however, the cost lump sums must be settled in accordance with the Court Allowances Act which may result, all told, in increased costs.

As a result of the introduction of a new criminal offence, the Federal State budgets may incur procedural and enforcement costs, the precise level of which cannot be quantified in greater detail. In any event, the Federal Government shall incur a limited amount of additional expenditure. Any increased demand for equipment and personnel can be offset within existing capacity and available funds and must be balanced, in terms of funds and job numbers, in the respective detailed plan 07.

Otherwise, no additional costs shall be borne by businesses, in particular, small- and medium-sized enterprises. Effects on individual prices and the general price level, in particular the consumer price level, are not anticipated.

5. Other legal consequences

In terms of content, the regulations refer to men and women alike and take into account the provision under § 1(2) of the Federal Equal Opportunities Act, according to which Federal Government laws, regulations and administrative provisions are designed to give expression to the equal status of men and women in linguistic terms too. No implications for equality policy are anticipated.

Demographic repercussions or those from the point of view of consumer policy are not obvious.

VI. Time limitation; evaluation

Imposing a time limit on the regulations is not appropriate. An evaluation is not provided for at the present moment. The draft does make provision, however, for a statistical recording of the investigative measures undertaken which will facilitate a subsequent evaluation. Should a further need for change be identified, the criminal prosecution authorities shall inform the justice department.

B. Specific Part

Re Article 1 (Amendment of the Code of Criminal Procedure)

Re point 1 (Table of contents)

The Table of contents with section designations in the Code of Criminal Procedure which is newly introduced by means of the Act of … [insert here: Federal Law Gazette …] is supplemented by the newly established provisions.

Re point 2 (§ 100g of the Draft Code of Criminal Procedure)

In its judgment relating to the retention of data, the Federal Constitutional Court declared §§ 113a and 113b of the Telecommunications Act, and also § 100g(1) sentence 1 of the Code of Criminal Procedure, insofar as traffic data as per § 113a of the Telecommunications Act could be collected in accordance with these provisions, to be invalid on account of an infringement of Article 10(1) of the Basic Law. Furthermore, the Federal Constitutional Court did not object to the provision under § 100g of the Code of Criminal Procedure in its judgment, especially not to the collection of traffic data which the telecommunications companies store for commercial purposes in accordance with §§ 96 *et seq.* of the Telecommunications Act. The incorporation of a storage obligation in the Telecommunications Act does, however, necessitate, a fundamental reorganisation of § 100g of the Code of Criminal Procedure in order to ensure compliance with the stipulations under constitutional and European law which are associated with such a storage obligation. This includes differentiated and systematic provisions relating to the obligations to notify and the possibilities of subsequent legal redress (§ 101a(3) to (4) of the Draft Code of Criminal Procedure).

Re paragraph 1

§ 100g(1) of the Draft Code of Criminal Procedure applies exclusively to the collection of traffic data which the providers of publicly available telecommunications services may store for commercial purposes in accordance with the definitive catalogue in § 96(1) of the Telecommunications Act. Deletion of the words "without the knowledge of the person concerned either" clarifies the fact that traffic data collection in accordance with § 100g of the Draft Code of Criminal Procedure is essentially not a surreptitious measure. Where possible, the data must be used in an open manner. Moreover, the requirement for an appropriate balance between data collection and the importance of the matter is also specifically incorporated in relation to the cases under paragraph 1 point 1.

Location data may only be collected in accordance with this paragraph in relation to traffic data which accumulates in future or in real time, and only in the case of sentence 1 point 1, if this is necessary for the purpose of investigating the facts of the case or for establishing the whereabouts of the suspect. A distinction is thereby drawn with regard to the particularly sensitive location data which essentially facilitates the compilation of movement profiles: Location data that has not been stored shall still be available to the authorities to the same extent as prior to the redrafting. Access to the stored data shall only continue to be possible under the conditions laid down in paragraph 2.

Re paragraph 2

§ 100g(2) of the Draft Code of Criminal Procedure regulates the collection of traffic data which must be stored on a compulsory basis in accordance with § 113b of the Draft Telecommunications Act. A restriction compared with paragraph 1 follows, on the one hand, from the fact that this data may only be collected in the case of the specific, particularly serious crimes listed in detail.

In their judgments relating to the retention of data, both the Federal Constitutional Court and the Court of Justice of the European Union have restricted use of the stored traffic data relating to criminal prosecution to the sphere of serious crime:

As regards criminal prosecution, this means that retrieval of the data at least presupposes the suspicion that a serious crime has been committed as justified by certain facts. As to which criminal offences are to be covered by this shall be stipulated conclusively by the legislator with the obligation concerning data storage. There is a certain margin of discretion in this regard. In this regard, the legislator can either revert to existing catalogues or create a separate catalogue, for example, in order to include criminal offences for which the telecommunications traffic data has special significance. Classification of an offence as serious must, however, find objectified expression in the penal provision – especially, for instance, by means of the penalties thereunder (cf. Federal Constitutional Court Decisions 109, 279 <343 *et seq.*, in particular 347 f.>). A general clause or merely making reference to criminal offences of major importance are not sufficient, however (Federal Constitutional Court Decisions 125, 260 <328 f.>).

The Court of Justice of the European Union has demanded objective criteria which restrict intervention under Articles 7 and 8 of the Charter of Fundamental Rights to criminal offences which can be regarded as sufficiently serious with regard to the fundamental rights concerned in order to justify the intervention (Digital Rights judgment, C-294/13 and C-594/12, recital 60).

In accordance with these stipulations, the traffic data stored in accordance with § 113b of the Draft Telecommunications Act may only then be collected if certain facts create the suspicion that someone, as perpetrator or accessory, has committed a particularly serious criminal offence as indicated in the catalogue under § 100g(2) sentence 2 of the Draft Code of Criminal Procedure, including in a given case, or has attempted to commit such an offence in cases in which such attempt constitutes an offence.

By way of a manifestation of the principle of proportionality, provision is also made for a subsidiarity clause in keeping with § 100g(1) sentence 1 of the Draft Code of Criminal Procedure, according to which this data may only be collected if this is necessary for the purpose of investigating the facts of the case and the collection of the data are in a reasonable proportion to the importance of the matter.

As regards the enumerative list of the criminal offences to be classified as particularly serious under § 100g(2) sentence 2 of the Draft Code of Criminal Procedure, recourse was made to a subset of the crimes included in the catalogue under § 100a(2) of the Code of Criminal Procedure. The Federal Constitutional Court has determined that the catalogue of criminal offences under § 100a(2) of the Code of Criminal Procedure complies with the constitution in its decision of 12 October 2011 (2 BvR 236/08). In this decision, the court rejected constitutional grievances by means of which, *inter alia*, a breach of fundamental rights by § 100a(2) of the Code of Criminal Procedure was rebuked (Federal Constitutional Court Decisions 129, 208 <241 f.>).

The catalogue was significantly reduced with respect to the high level of relevance in terms of fundamental rights of the retrieval of data stored on a compulsory basis. The catalogue includes criminal offences which assist in the combating of terrorism or the protection of personal objects of legal protection, in particular the protection of life and limb, freedom and sexual self-determination. Particularly serious crimes where the stored traffic data can prove to be particularly valuable, based on criminological experience, are also covered.

According to paragraph 2, location data to establish the whereabouts of the suspect may be collected under the preconditions mentioned therein.

Re paragraph 3

Paragraph 3 contains a special provision relating to radio cell inquiries. These radio cell inquiries do not involve location data collection. Instead, in the case of such an enquiry, all traffic data which has accumulated in the course of such an inquiry is collected in order to determine which mobile devices had to be assigned at a specific time of the radio cell in question. The draft Act includes a legal definition of the term "radio cell inquiry" and states their preconditions. In this way, a legally clear enabling provision is created for radio cell inquiries.

Radio cell inquiries where data stored in accordance with § 96(1) of the Telecommunications Act is to be accessed are made on the basis of paragraph 3 sentence 1. The preconditions under paragraph 1 point 1 must exist. Moreover, the data must be collected in a reasonable proportion to the importance of the matter (point 2). Finally, the investigation of the facts of the case or the establishment of the whereabouts of the suspect in another way must be futile or considerably more difficult (point 3).

These tighter preconditions governing admissibility of radio cell inquiries compared with the current status are necessary in order to reduce the disproportionate infringement of a great number of those affected. As a result of radio cell inquiries, traffic data pertaining to third parties in particular, i.e. those persons who, without being a suspect or conveyor of (illegal) communications, have communicated using their mobile telephone in the radio cell being inquired about, is collected unavoidably. Consideration must already be given under existing law in connection with the order as to the extent to which third persons are affected by a radio cell inquiry. In a given case therefore, the measure can be restricted further in terms of time and place, for reasons of proportionality, or must be stopped if such a restriction is not possible and the extent to which third parties are affected seems disproportionate (cf. *Bundestag* document no. 16/5846, p. 55). At the same time, account is to be taken in particular of the principle of proportionality by means of clarification of the requirements concerning the radio cell inquiry order, so as to prevent a situation from the outset whereby traffic data of non-participants is collected over and above the extent necessary for criminal prosecution and, at the same time, movement profiles could be compiled by the criminal prosecution authorities. As regards the authorities giving the orders, their awareness is to be increased in reference to this such that in the context of the proportionality test, special consideration is required in particular with respect to the fact that as a result of the radio cell inquiry, traffic data pertaining to third parties is unavoidably collected on a regular basis.

Radio cell inquiries where data stored in accordance with § 113b of the Draft Telecommunications Act is to be accessed are made on the basis of paragraph 3 sentence 2, in conjunction with paragraph 2.

The previous provision concerning the organisation of the radio cell inquiry in § 100g(2) sentence 2 of the Code of Criminal Procedure can now be found in § 101a(1) sentence 3 of the Draft Code of Criminal Procedure.

Re paragraph 4

Both the Federal Constitutional Court and the Court of Justice of the European Union (Digital Rights judgment, C-294/13 and C-594/12, recital 58) have emphasised that the proportionality of traffic data storage presupposes special regulations designed to protect individuals who are subject to professional obligations to maintain strict confidentiality.

Alongside the provision under § 113b( ) of the Draft Telecommunications Act, which excludes the calls stated in § 99(2) sentence 2 of the Telecommunications Act from the storage obligation under § 113b(2) of the Draft Telecommunications Act, paragraph 4 therefore makes provision for a general ban on the collection of traffic data which is directed against persons mentioned in § 53(1) points 1 to 5. The provision under

§ 160a(1) concerning the retrieval of data stored in accordance with § 113b of the Draft Telecommunications Act is thereby extended to the extent that a ban on collection exists with respect to all the professional groups stated in § 53(1).

It is not feasible to already exempt all individuals with a duty of professional secrecy from having their traffic data stored. To this end, all telecommunications providers, of which there are approximately 1 000 in Germany, should be notified regarding which individuals have a duty of professional secrecy within the meaning of § 53 of the Code of Criminal Procedure. This list must be updated on a continuous basis. In the event of the person concerned giving their consent, the creation, forwarding and updating of this list also involves a considerable risk of abuse. Added to this is the fact that in many cases, individuals with a duty of professional secrecy do not have static but dynamic IP addresses at their disposal, meaning that a list of the addresses used could not be compiled at all. Superior protection is therefore afforded by a provision which excludes the use of the stored data. This safeguarding mechanism has also proven itself elsewhere in the Code of Criminal Procedure.

Re paragraph 5

The provision in paragraph 5 complies with current law (§ 100g(3)) and clarifies the fact that the collection of traffic data observes general regulations, i.e. §§ 94 *et seq.* of the Code of Criminal Procedure in particular, if it takes place, for instance, by seizing objects (e.g. electronic storage media, but also itemised bills in paper form) following the conclusion of the communication process in a manner other than by sending an information injunction to the provider of publicly available telecommunications services.

Re point 3 (§ 100j of the Draft Code of Criminal Procedure)

The proposed addition to § 100j(2) of the Code of Criminal Procedure makes provision for the fact that as regards inventory data information relating to IP addresses, traffic data stored in accordance with § 113b of the Telecommunications Act may be used.

§ 100j of the Code of Criminal Procedure does not require further supplements. In particular, paragraph 4 thereof already contains provisions regarding notification of the person concerned and thereby also corresponds to the stipulations under constitutional law inasmuch as in future, information may be exchanged in accordance with § 100j(2) of the Code of Criminal Procedure on the basis of data stored in accordance with § 113b of the Draft Telecommunications Act (IP addresses).

Re point 4 (§ 101 of the Draft Code of Criminal Procedure)

This constitutes a consequential amendment which follows from qualification of the traffic data inquiry as an overt measure.

Re point 5 (§§ 101a and 101b of the Draft Code of Criminal Procedure)

Re § 101a of the Draft Code of Criminal Procedure

By means of the Act re-regulating telecommunications monitoring and other covert investigative measures and transposing Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette I p. 3198), the legislator summarised all those procedural provisions, which, hitherto, had all been regulated separately each time, under § 101 of the Code of Criminal Procedure in relation to the investigative powers as per §§ 98a, 99, 100a, 100c, 100f to 100i, 110a and 163d *et seq.* thereof. The provision thereby governs in a consistent manner all specific covert measures including, *inter alia*, identification requirements, obligations to notify and their deferment, in addition to judicial reviews.

Moreover, additional legal protection is granted in order to reinforce the fundamental right to a fair hearing in accordance with Article 103(1) of the Basic Law and the requirement of ensuring effective legal protection as per Article 19(4) of the same.

For systematic reasons, the collection of traffic data in accordance with § 100g of the Draft Code of Criminal Procedure shall be removed from the scope of this uniform provision concerning procedural regulations which safeguard fundamental rights in the case of covert investigative measures since the provision henceforth complies with the stipulations of the Federal Constitutional Court which had specified that in future, the collection of traffic data shall essentially be organised as an overt measure in any case for the area of criminal prosecution: "Among the transparency requirements is the principle of openness when collecting and utilising personal data. Using the data without the knowledge of the person concerned is only then permitted under constitutional law if the purpose of the investigation, a process which data retrieval assists in, is otherwise thwarted. The legislator may accept this in principle for protecting against threats and the performance of tasks by the intelligence services. In comparison, the principle of openness when collecting and utilising data also comes into consideration within the framework of criminal prosecution (cf. § 33(3) and (4) of the Code of Criminal Procedure). In this regard, investigative measures are also otherwise partly carried out with the knowledge of the accused and in their presence (cf., for example, §§ 102, 103 and 106 of the Code of Criminal Procedure). In principle, the person concerned must be notified accordingly prior to the retrieval or transmission of their data. Provision may only be made for the data to be used in a clandestine manner if this is necessary and ordered by a judge in a given case." (Federal Constitutional Court Decisions 125, 260 <335 f.>).

In § 101a of the Draft Code of Criminal Procedure, the procedure for collecting traffic data are adapted to the procedure for ordering overt measures.

Re paragraph 1

Paragraph 1 contains the judge's discretion which is important for traffic data collections pursuant to § 100g. At the same time, a distinction is drawn between the nature of the stored data. In paragraph 1 sentence 1, reference is made, as before, to § 100a(3) and § 100b(1) to (4) of the Code of Criminal Procedure. By way of deviation from this, in paragraph 1 sentence 2, in the cases referred to in § 100g(2), also in conjunction with § 100g(3) sentence 2, § 100b(1) sentences 2 and 3 are exempted from application. With respect to the collection of data to be stored on a compulsory basis, the possibility of an urgent order from the public prosecutor's office where danger is imminent does not therefore exist. Under sentence 1, this possibility only exists for traffic data collections as per § 100g(1) and (3) sentence 1. For all radio cell inquiries according to § 100g(3), a special provision is laid down in paragraph 1 sentence 3. By way of deviation from § 100b(2) sentence 2 point 2, the call number or another identifier of the line to be monitored or the terminal device do not have to specified in this regard unless it emerges from certain facts that this is assigned to another terminal device at the same time. Instead, it is sufficient to declare the telecommunication as being geographically limited, short-term and sufficiently specific.

§ 101a(1) point 1 of the Draft Code of Criminal Procedure fulfils the stipulation of the Federal Constitutional Court whereby in the order, the types of data to be transmitted according to the principle of proportionality must be designated in an adequately selective and clear manner. The Court of Justice of the European Union also considered the preconditions under procedural law concerning access on the part of the competent national authorities to data and its subsequent use to be necessary (Digital Rights judgment, C-294/13 and C-594/12, recital 61). The new regulation also makes provision for the fact that the period for which the data are to be transmitted must be specified clearly. This serves to clarify the fact that time-related data must be provided not only when collecting data which accumulates in the future, as is provided for under § 100b(2)

sentence 2 point 3, but that the period of time for which it is to be collected must be designated precisely when collecting data that has already been stored. This is designed to ensure that all existing data are not collected across the board without a corresponding need but that its collection is limited from the outset to those periods which are relevant to the investigation.

§ 101a(1) point 2 of the Draft Code of Criminal Procedure makes provision for the fact that the party obligated to provide information in accordance with § 100b(3) sentence 1 must also advise as to which parts of the data transmitted by the party originate from the data to be stored in accordance with § 113b of the Draft Telecommunications Act. This communication is necessary for the special identification stipulated by § 101a(3) of the Draft Code of Criminal Procedure and also for the purpose of statistics according to § 101b of the aforementioned code.

Re paragraph 2

As regards all the measures under § 100g of the Draft Code of Criminal Procedure and the extension thereof, paragraph 2 makes provision for a qualified obligation to state reasons on the basis of § 81g(3) sentence 5 and § 100d(3) sentences 1 and 2 of the Code of Criminal Procedure.

The clear stipulations regarding justification and the appropriateness of the measure, including with regard to the scope of the types of data to be collected and the period of time for which it is to be collected, define in more precise terms the requirements already arising from § 34 of the Code of Criminal Procedure regarding the judicial order for traffic data collection and the extension thereof. The authorities giving the orders are especially encouraged to express the definitive aspects of proportionality in the decision for an order and extension in a transparent and comprehensible manner. In principle, only specific location data are to be retrieved so as not to compile any superfluous movement profiles if these are not required in a given case, e.g. in order to clear up a serial act or to attain clues as to movements specified by the suspect. As a result of such a qualified obligation to state reasons, reinforcement of the judge's discretion, improved legal protection for those persons affected by the measure (this applies, above all, to third parties who are unavoidably impacted) and improved reviewing of the decision in the event of an *a posteriori* control which the courts can exercise can be achieved (cf. *Bundestag* document no. 15/4522, p. 17, for § 100d(3) of the Code of Criminal Procedure).

Re paragraph 3

The stipulation under sentence 1, according to which personal data which has been collected by means of measures in accordance with § 100g must be identified accordingly, corresponds to § 101(3) sentence 1 of the Code of Criminal Procedure.

Moreover, paragraph 3 sentence 1 prescribes that personal data which has been collected as a result of measures under § 100g, must be evaluated forthwith so as not to perpetuate and thereby deepen the intrusion associated with the continual storage of the data. The traffic data collected must be deleted forthwith in accordance with § 101(8) of the Code of Criminal Procedure if it is no longer required for prosecution purposes or for any judicial review. In accordance with paragraph 3 sentence 1, this also applies to traffic data which was not stored pursuant to § 113b of the Telecommunications Act because it is also necessary to avoid in this respect a perpetuation of the intrusion associated with the continual storage of the data and this facilitates, moreover, consistent and thereby easier handling in practice.

Paragraph 3 sentence 2 stipulates that it must be noticeable whether the data in question was stored in accordance with § 113b of the Draft Telecommunications Act. This particular identification requirement is necessary so as to be able to guarantee the narrow

purpose limitation principle which applies to this data in a comprehensive manner and be able to ensure that the data are used exclusively to carry out tasks on whose account access to this data would also be permitted directly.

Paragraph 3 sentence 3 provides that identification must be maintained in the case of transmission to other authorities.

Through its reference to § 101(8) of the Code of Criminal Procedure, paragraph 3 sentence 4 adopts the stipulations relating to deletion, the importance of deletion and blocking already applicable hitherto to traffic data as well.

Re paragraph 4

Paragraph 4 serves to transpose the stipulation of the Federal Constitutional Court, according to which a transfer to other authorities of the personal data stored in accordance with § 113b and transmitted within the framework of traffic data collection as per § 100g(2), also in conjunction with § 100g(3) sentence 2, may only be envisaged under law if this happens with a view to carrying out tasks on whose account access to this data would also be permitted directly (Federal Constitutional Court Decisions 125, 260 <333>). The provision prevents a circumvention of the restrictive regulations governing use in § 113c(1) of the Draft Telecommunications Act. It is guided by § 100d(5) of the Code of Criminal Procedure.

Sentence 1 governs the further use of personal traffic data collected in accordance with § 100g(2), also in conjunction with § 100g(3) sentence 2, of the Draft Code of Criminal Procedure, for other purposes. It clarifies the fact that further use of the data are subject to the same bans on utilisation as in the main proceedings. Any purpose-redesignating use of the data are only permitted if the data may also be utilised in the main proceedings.

According to point 1, further use of the data in the other criminal procedure is only permitted if it is required in order to investigate a criminal offence within the meaning of § 100g(2) sentence 2 of the Draft Code of Criminal Procedure. The presence of such a criminal offence is not sufficient, however, to justify the further use of the knowledge acquired. Instead, the other preconditions under § 100g(2) of the Draft Code of Criminal Procedure must be present. This is taken into account by means of the wording whereby the measure could be arranged in the other criminal procedure.

Point 2 regulates the further use of personal traffic data collected in accordance with § 100g(2) of the Draft Code of Criminal Procedure for preventive purposes. This is only permitted for the purpose of averting specific risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings (Federal Constitutional Court Decisions 125, 260 <332>). A transfer of data collected for repressive purposes to authorities with preventive functions is thereby also only permitted within the physical limits laid down by § 113(1) point 2 of the Telecommunications Act. The authority responsible for using the data further must have an enabling law which allows retrieval (double-door model).

Re paragraph 5

Paragraph 5 governs the reverse case of the further use in criminal proceedings of traffic data collected on a preventive basis which was stored in accordance with § 113b of the Draft Telecommunications Act. Further use [of the data] is only permitted if a measure as per § 100g(2), also in conjunction with § 100g(3) sentence 2, could be arranged in the criminal procedure.

Re paragraph 6

The court involved in an application to issue an order in accordance with § 100g of the Draft Code of Criminal Procedure must give the person concerned an opportunity for a fair hearing already prior to the decision being taken in accordance with § 33 of the Code of Criminal Procedure. The hearing according to § 33(4) sentence 1 of the Code of Criminal Procedure can only be refrained from if the preceding hearing were to jeopardise the purpose of the order. This must be justified on a case-by-case basis.

If the court issues the order applied for, as it requires execution on a regular basis, this shall be forwarded to the public prosecutor's office in accordance with § 36 of the Code of Criminal Procedure which shall then make the necessary arrangements. This shall also include informing the persons concerned in accordance with § 101a(6) of the collection of the traffic data (which is pending). If reasons exist which preclude a notification being made at this time, it must be deferred with the court's consent. In such a case, the court will have issued an order on a regular basis without a prior hearing with the person concerned. In practice, it may therefore be advisable to already present the application for consent to defer the notification at the same time as the application ordering traffic data collection.

§ 101a(6) makes reference to § 101(4) to (7) of the Code of Criminal Procedure as regards notification and legal redress. In reference to the stipulations of the Federal Constitutional Court, by way of deviation from § 101 of the Code of Criminal Procedure, it is stipulated that refraining from a notification as per § 101(4) sentence 3 of the Code of Criminal Procedure requires a judicial order (§ 101a(5) point 1) and that the first-time deferment of a notification in accordance with § 101(5) sentence 1 of the Code of Criminal Procedure also requires a judicial order (§ 101a(5) point 2).

Re § 101b of the Draft Code of Criminal Procedure

The new § 101b, as a consequential amendment, supersedes the current stipulations in § 100g(4) of the Code of Criminal Procedure regarding the statistical recording of traffic data collection on the basis of § 100g of the aforementioned code. By means of the reference to § 100b(5) of the Code of Criminal Procedure, it is stipulated that the Federal States and the Federal Public Prosecutor must report to the Federal Office of Justice every calendar year regarding the measures ordered within its area of responsibility so that the latter may draw up a corresponding overview regarding publication on the internet. The statistics are designed to strengthen the transparency of the measures in accordance with § 100g and facilitate their evaluation. The reference to § 100b(5) of the Code of Criminal Procedure corresponds to the reference in the current § 100g(4) of the Code of Criminal Procedure and stipulates under point 1 that the Federal States and the Federal Public Prosecutor must report to the Federal Office of Justice every calendar year regarding the measures ordered within its area of responsibility in accordance with paragraphs 1, 2 and 3 so that the latter may draw up a corresponding overview regarding publication on the internet. Moreover, point 2 stipulates that the number of orders to be raised, differentiated according to points 2a to 2d, must be indicated separately for the areas of fixed network, mobile and internet services and subdivided each time according to the number of past weeks for which the collection of traffic data were ordered, measured each time from the date of the order.

Re point 6 (§ 160a of the Draft Code of Criminal Procedure)

Re letter a

This constitutes a consequential amendment relating to Article 3 point 2. Since the receipt of stolen data constitutes a criminal offence after the fact, the corresponding provisions in the Code of Criminal Procedure must be adapted.

Re letter b

This constitutes a consequential amendment which follows from the provision concerning bans on collection and utilisation designed to protect the persons in paragraph 4 who are authorised to refuse to give testimony as referred to in § 53(1) of the Code of Criminal Procedure.

Re point 7 (§ 304 of the Draft Code of Criminal Procedure)

This constitutes a consequential amendment which follows from the removal of § 100g from the clandestine investigative measures under § 101 of the Code of Criminal Procedure.

Re point 8 (§ 477 of the Draft Code of Criminal Procedure)

This constitutes a consequential amendment which follows from the special provision under § 101a(4).

Re point 9 (§§ 3, 60, 68b, 97, 102 and 138a of the Draft Code of Criminal Procedure)

This constitutes a consequential amendment relating to Article 5 point 2. Since the receipt of stolen data constitutes a criminal offence after the fact, the corresponding provisions in the Code of Criminal Procedure (§ 3, § 60 point 2, § 68b(1) sentence 4 point 1, § 97(2) sentence 3, § 102, § 138a(1) point 3 of the Code of Criminal Procedure) must be adapted.

Re Article 2 (Amendment of the Telecommunications Act)

Re point 1 (Table of contents)

The Table of contents must be adapted in line with the headings under §§ 113a to 113g of the Draft Telecommunications Act.

Re point 2 (§§ 113a to 113g of the Draft Telecommunications Act)

Re § 113a of the Draft Telecommunications Act

This provision describes the circle of parties obligated to store. According to paragraph 1 sentence 1, the storage obligations are aimed at those parties which provide publicly available telecommunications services within the meaning of § 3 point 6a) of the Telecommunications Act, i.e. not at those parties which merely play a part in this. Providers are characterised by the fact that a separate telecommunications connection for autonomous use which is generally laid for an indefinite period is relinquished to customers on a regular basis. Consequently, providers which only allow their customers short-term use of the telecommunications connection, e.g. hotel, restaurant and café operators, who make telephone or internet use available to their customers (see Notification No. 149/2015 in the Official Journal of the Federal Network Agency for a more detailed definition of the term "provision") are not under any obligation. Compared with § 113a(1) sentence 2 of the previous version of the Telecommunications Act, the provision under sentence 2 henceforth covers both the case where the provider of publicly available telecommunications services does not itself generate or process any of the data to be stored in accordance with this provision and also the case where the provider itself generates and processes some, but not all, of the data to be stored. The obligation whereby retention as per sentence 2 is guaranteed only exists, however, if the data are generated or processed during provision of the service.

Paragraph 2 of the Act also makes provision for the possibilities of compensation for enterprises which are able to furnish proof of undue hardship when implementing the retention obligation. Corresponding applications are reviewed by the Federal Network Agency, in which connection the applicants must demonstrate that the implications of the storage obligation for their enterprise could have a choking effect.

Re § 113b of the Draft Telecommunications Act

The provision under § 113b of the Draft Telecommunications Act serves as a key provision for transposing the stipulations of the Federal Constitutional Court and the Court of Justice of the European Union by determining the recipients and the basic preconditions of the storage obligations, stipulating the categories of data to be stored and the retention period, and lays down guidelines as to how the data are to be stored and deleted.

Re paragraph 1

Paragraph 1 contains the obligation concerning data storage, differentiated between according to call detail records and location data. In the case of call detail records, a retention period of 10 weeks is specified (point 1); location data (§ 113b(4) of the Draft Telecommunications Act) may only be retained for 4 weeks (point 2). This corresponds to the requirement for a provision which is as considerate as possible as regards fundamental rights. The retention period is sufficient in order to ensure that the relevant data are available in the predominant number of requests. By way of deviation from § 113a of the previous version of the Telecommunications Act, the data must be stored exclusively in Germany. Fulfilment of the storage obligation as a result of storing the data in another Member State of the European Union is no longer envisaged.

Limiting data retention to Germany constitutes a restriction on the freedom to provide services within the meaning of Article 56 of the Treaty on the Functioning of the European Union. Such a restriction is justified if it is necessary in order to satisfy overriding reasons relating to the public interest and provided it is also proportionate. These preconditions are in place. Restricting data retention to Germany is necessary in order to guarantee the requirements of data protection under Basic Law and data security, to protect effectively the data retained against any unauthorised access attempt and any unauthorised use, and so that an independent body is able to monitor the situation in a timely and efficient manner.

Only in Germany can the requirements included in §§ 113c *et seq.* of the Draft Telecommunications Act, in particular those pertaining to data usage and security, be guaranteed and reviewed in a comprehensive manner. As regards storage in other European countries, it could not be excluded that, contrary to the rigorous restriction on use in § 113c of the Draft Telecommunications Act, the foreign state shall have access to the data stored on its sovereign territory in accordance with its (national) law, something which, given recent experience, seems to be more than just a theoretical risk.

Moreover, the German public bodies in other EU Member States which are concerned with reviewing compliance with security standards and data protection would not have any direct and equally effective opportunities to conduct reviews since every supervisory authority is limited to its own sovereign territory when exercising supervisory powers. Indeed, as regards cross-border data processing, the German authority could ask the supervisory authority in another Member State, through a process of mutual assistance, to exercise its powers on its own soil (Article 28(6) sentence 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23 November 1995, p. 31). In view of the scope of the test obligations and the fact that it does not involve a one-off review of a provider but the

execution of permanent tasks (for example, when adapting the security concepts in line with the respective state of the art), however, this appears to be insufficiently effective. In the case of individual complaints moreover, it would not be guaranteed that the review takes place sufficiently quickly.

Re paragraph 2

Paragraph 2 sentence 1 sets out the individual storage obligations for providers of publicly available telephony services and covers characteristics such as fixed network, mobile and internet telephony. Sentence 2 clarifies the fact that these storage obligations shall apply accordingly when providing voice short message services (SMS) and Multimedia message services (MMS), along with similar messages (e.g. EMS), in which connection the exact dates and times to be stored relate to the sending and receipt of the message, in the absence of an existing connection. Sentence 3 extends the storage obligation to unanswered (i.e. not accepted) calls, or to those which are unsuccessful on account of network management interference, provided the telephony provider stores or logs the traffic data for the purposes mentioned in § 96(1) sentence 2. By means of this provision, which corresponds to § 113a(5) of the previous version of the Telecommunications Act, cases are covered, for example, where a subscriber is informed by their service provider, via text message, that a call destined for their line was not accepted, for instance, because the line was engaged or, at the time of the call, the mobile telephone was situated outside the area of coverage of the radio cell.

Regarding the content and scope of the storage obligations in paragraph 2 sentence 1, reference is made to the following in particular:

Point 1 ensures that – even in the event of a call being redirected or forwarded – the call numbers or other ID codes that are required in the area of telephony for identifying the communication subscribers are available.

Point 2 guarantees the precise determinability of a telecommunication that has taken place from the point of view of time.

Point 3 concerns the situation whereby other services may be utilised in the context of the telephony service. In this case, information regarding which service was used during the respective telecommunications process must also be stored (in ISDN, for instance, voice, fax or data transfer; in mobile telephony, for instance, the sending of SMS messages or multimedia data [MMS]).

Point 4 describes special storage guidelines for the area of mobile telephony.

– According to letter a, the international identifiers for mobile subscribers for the calling and the called line (what are known as IMSIs) must be stored.

– According to letter b, the international identifiers for the calling and the called terminal equipment (what are known as IMEIs) must be stored.

– According to letter c, when utilising anonymous telephony services paid for in advance, the time when the service is first activated must be stored. If a prepaid card such as this is activated when a call is made to the telecommunications service provider, this data are already covered by points 1, 2 and 4 letters a and b, meaning that on the basis of this activation process, letter c shall not result in any additional data storage. If the service is activated in a way whereby traffic data are neither generated nor processed, as may be the case if activation takes place as a result of instant online registration when the contract is concluded by an employee of the provider of publicly available telecommunications services, this does not justify any storage obligation in accordance with paragraph 1 sentence 1.

Point 5 governs the obligation to store the IP addresses of the calling and called line for the area of internet telephony in order to allow determination of the call which was the destination or origin of an internet phone call. In the case of telephony services over the internet, the assigned user IDs must also be stored.

Re paragraph 3

Paragraph 3 sets out the individual storage obligations for providers of publicly available internet access services. The addresses accessed on the internet (so-called URLs [Uniform Resource Locators]) shall not be stored. Traceability shall therefore also follow on the basis of the internet data to be stored, not the "surfing habits" of internet users as a whole.

As is the case with § 113b(2) point 5 of the Draft Telecommunications Act, in order to better facilitate the practice of the tracing and identification of the source of a communications process, in accordance with § 113b(3) point 2, in addition to the call identifier via which the internet is utilised, the assigned user ID must also be stored.

Re paragraph 4

According to paragraph 4, the location data of the calling and called line at the start of the call, i.e. the specific radio cell designations via which the telecommunications subscribers are supplied when establishing a connection, must be stored for 4 weeks. When utilising publicly available internet access services through mobile communications, the designation of the radio cell used at the start of the internet connection must be stored.

In addition, paragraph 4 sentence 3 determines that data must also be retained from which follows the geographical location and the main beam directions of the antennas supplying the respective radio cell. This provision, which takes up § 113a(7) of the previous version of the Telecommunications Act, concerns data relating to the network planning of mobile network operators, i.e. it does not therefore govern the storage of traffic data. The information is required in order to be able to assign to specific geographical areas the radio cell designations to be stored in accordance with paragraph 1 point 4, as well as in relation to mobile, publicly available internet access services, which are regularly only presented in alphanumeric form and, as such, are largely useless for investigation purposes. Since these radio cell designations are not permanently assigned by the providers of publicly available telecommunications services on account of developing network structures and, for instance in the case of large-scale events, other radio cells are frequently only established on a short-term basis, it is necessary to ensure that information regarding the geographical assignment can be provided for the duration of the storage obligation in accordance with this provision. Specifying the main beam directions of the individual antennas serves to facilitate a more precise determination of the location from or to which a telecommunications connection was established.

Re paragraph 5

The provision under paragraph 5 clarifies the fact that the content of communications, data pertaining to websites visited and data from electronic mail services may not be stored in accordance with this regulation.

Re paragraph 6

According to the stipulation of the Federal Constitutional Court in its judgment relating to the retention of data, by way of emanation of the principle of proportionality, a fundamental ban on transmission is required under constitutional law "in relation to a tightly-knit circle of telecommunication links which rely on exceptional confidentiality" (Federal Constitutional Court Decisions 125, 260 <334>). Typical examples – according to

the Federal Constitutional Court – include the telecommunication links stated in § 99(2) sentence 1. Pursuant to § 99(2) sentence 1 of the Telecommunications Act, itemised bills may not be indicative of calls made to lines of persons, public authorities and organisations working for the church or in the social domain, who or which offer counselling wholly or predominantly by telephone to callers in emotional or social distress who remain essentially anonymous and where these individuals themselves, or the employees of these authorities and organisations, are subject to other non-disclosure obligations in this respect. The draft Act goes beyond the stipulations of the Federal Constitutional Court and does not preclude just transmission but also data storage. In this regard, the provisions under § 99(2) shall apply accordingly to the inclusion of these organisations in lists which are maintained and updated by the Federal Network Agency.

Re paragraph 7

The provision in paragraph 7 is designed to ensure that the data are stored by the obligated parties in a way that permits effective and rapid research so that requests for information can be answered immediately.

Re paragraph 8

Paragraph 8 stipulates that the traffic data stored on the basis of § 113b of the Draft Telecommunications Act must be deleted forthwith, but at the latest within 1 week of the lapsing of the retention period under paragraph 1 sentence 1, or the deletion of this data must be guaranteed. The data must be deleted in accordance with the state of the art, in connection with which the catalogue of requirements as per § 113f of the Draft Telecommunications Act will provide guidance. The deletion of the data must be logged in accordance with § 113e(1) of the Draft Telecommunications Act.

Re § 113c of the Draft Telecommunications Act

This provision governs the use of the traffic data stored in accordance with § 113b of the Draft Telecommunications Act and includes a narrow purpose limitation principle.

Re paragraph 1

According to paragraph 1 point 1, the data stored on the basis of § 113b of the Draft Telecommunications Act may be transmitted to a criminal prosecution authority if this authority demands transmission by invoking a provision of the law which allows it to collect the data referred to in § 113b of the Draft Telecommunications Act. The criminal prosecution authorities are only allowed to collect the stored data under the strict conditions laid down in § 100g(2) of the Draft Code of Criminal Procedure.

Paragraph 1 point 2 contains a provision concerning the transmission of data stored unconditionally to a public risk prevention authority. Such a transmission is subsequently permitted if a public risk prevention authority, i.e. the police, for example, demands this by invoking a legal right which allows it to collect the data stored unconditionally for the purpose of averting specific risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings. In this way, Federal State police authorities are afforded the opportunity to collect traffic data stored on a compulsory basis where corresponding enabling laws are available.

Paragraph 1 point 3 contains a provision for those cases where the data stored on a compulsory basis may be consulted by the provider of publicly available telecommunications services in order to furnish inventory data information as per § 113(1) sentence 3 for dynamic IP addresses.

This shall not apply to the prosecution or prevention of administrative offences. The use of data stored by the providers of publicly available telecommunications services in relation to inventory data information is also permitted, in principle, if the information assists in the prosecution or prevention of administrative offences (§ 113(2) sentence 1 of the Telecommunications Act). § 46(2) of the Act on administrative offences makes provision, however, for the fact that requests for information relating to circumstances which are subject to postal and telecommunications secrecy are not permitted. In its decision of 24 January 2012 (1 BvR 1299/05), the Federal Constitutional Court determined that the identifying assignment of dynamic IP addresses has special similarities with specific telecommunications processes and comes under the scope of protection of Article 10(1) of the Basic Law (Federal Constitutional Court Decisions 130, 151 <181 f.>). The assignment of dynamic IP addresses in the context of inventory data information is therefore not permitted in relation to the prosecution of administrative offences.

Whether the authorities are entitled to direct a request within the meaning of points 1 to 3 to the provider of publicly available telecommunications services is not the subject of the provision under § 113c of the Draft Telecommunications Act, but is determined in accordance with the provisions of criminal procedure law, in this instance §§ 100g and 100j of the Code of Criminal Procedure, which are decisive for the criminal prosecution authorities. § 100j(2) of the Code of Criminal Procedure does not therefore make reference just to § 113(1) sentence 3 of the Telecommunications Act, but expressly includes § 113c(1) in order to justify the exchange of information from this data on the part of the authority submitting the request. The authorities must review under their own responsibility whether the preconditions for a transmission request are in place. In the case referred to in § 100g of the Code of Criminal Procedure, moreover, a corresponding judicial order must be obtained in principle. In this respect, the provider is assigned neither a substantial examination requirement nor the authority to conduct examinations.

These provisions comply with the stipulations of the Federal Constitutional Court (Federal Constitutional Court Decisions 125, 260 <329-332> and <355f> or, regarding indirect data use, <340-344, 356>).

Re paragraph 2

Paragraph 2 stipulates that the data stored on the basis of § 113b of the Draft Telecommunications Act by the providers of the telecommunications services may not be used for purposes other than those stated in paragraph 1 or for logging in accordance with § 113e of the Draft Telecommunications Act. Infringements of this obligation are punishable by a fine (§ 149(1) point 39 of the Draft Telecommunications Act). Even after the data are transmitted, its usage is subject to strict provisions. These provisions for the criminal prosecution authorities can be found in § 101a(4) of the Draft Code of Criminal Procedure.

Re paragraph 3

Strict requirements must also be imposed on the transmission of the data to the authorised individuals in order to guarantee the security of the data. This is done by also applying the measures regulated in § 110 of the Telecommunications Act to the transmission of the data stored in accordance with § 113b of the Draft Telecommunications Act. Reference is made to the stipulations under the statutory instrument pursuant to § 110(2) and the Technical Guideline as per § 110(3). The Federal Constitutional Court has requested furthermore that the data also be identified by the parties obligated in accordance with the Telecommunications Act (Federal Constitutional Court Decisions 125, 260 <346>) in order to ensure that the earmarking for a specific purpose can also be maintained while the data are being used further.

Re § 113d of the Draft Telecommunications Act

§ 113d of the Draft Telecommunications Act contains stipulations concerned with guaranteeing the security of the data stored in accordance with § 113b(2) to (4) of the Draft Telecommunications Act and is designed to transpose corresponding stipulations of the Federal Constitutional Court. The provision under § 113d, in conjunction with § 113f of the Draft Telecommunications Act, stipulates as binding a particularly high security standard. The technical substantiation of the standard specified is to be entrusted to the Federal Network Agency by means of the provision under § 113f of the Draft Telecommunications Act (cf. Federal Constitutional Court Decisions 125, 260 <325-327>).

Sentence 1 specifies that the data stored in accordance with § 113b(2) to (4) of the Draft Telecommunications Act is protected against unauthorised disclosure and use by means of state-of-the-art technical and organisational measures. These special security requirements do not extend to the data to be stored as per § 113b(4) concerning the geographical locations and the main beam directions of the antennas supplying the radio cells. Such data does not constitute traffic data and is independent from specific telecommunications processes, meaning that the particularly high level of protection covering data to be stored in accordance with § 113b(2) to (4) is not required in this respect.

Sentence 2 stipulates that the technical and organisational measures designed to protect the data to be stored in accordance with § 113b(2) to (4) cover the following in particular:

– the use of a particularly secure current cipher (point 1),

– storage in separate storage devices which are distinct from those used for standard operational tasks (point 2),

– storage provided with a high level of protection against internet-based access which shall be guaranteed in particular as a result of a physical separation from the internet (point 3),

– limiting access to the data processing equipment to persons who are specifically authorised (point 4), and

– ensuring application of the principle that two pairs of eyes are better than one as regards accessing the data (point 5).

The provision under point 3 is based on remarks made by the Federal Constitutional Court in its judgment relating to the retention of data, in which the expert remarks during the oral hearing as well as in the written submissions regarding possible instruments for raising security are drawn on (Federal Constitutional Court Decisions 125, 260 <325 f.>). Among the aspects mentioned in this connection are separate storage of the data on "computers which are isolated from the internet".

The principle that two pairs of eyes are better than one, as stipulated by point 5, says that access to the data stored unconditionally should not be possible for one person alone but that operating procedures are arranged in such a way that on a case-by-case basis, access to the data absolutely requires the involvement of at least one other person. It is conceivable, for example, that the inquiry data (for instance, reference number, name of the subscriber) is entered solely by an initial individual, although data stored unconditionally can only be released from the database by a second person employing password protection in a given case. In order to avoid an automated process with regard to the second individual, a code could be generated from the inquiry data entered by the first person which would be input, together with the password, by the second person in order to effect activation.

The measures must be arranged specifically according to the state of the art. Guidance is provided by the catalogue of requirements envisaged according to § 113f of the Draft Telecommunications Act in which it may be specified which cipher, which key size, which key management procedure or which organisational or technical arrangement of the principle that two pairs of eyes are better than one complies with the state of the art.

Re § 113e of the Draft Telecommunications Act

The provision under § 113e of the Draft Telecommunications Act is guided by the example of § 112(4) sentences 4 to 6 of the Telecommunications Act and transposes the corresponding stipulations of the Federal Constitutional Court regarding logging (Federal Constitutional Court Decisions 125, 260 <325 f>).

Re paragraph 1

Paragraph 1 specifies the logging in an audit-proof manner of any access to the data stored on the basis of § 113b of the Draft Telecommunications Act. The log is designed to enable the authority responsible for reviewing compliance with the provisions concerning the protection of personal data to check whether access has been effected in a lawful manner.

The term "access" includes all read-only access attempts, the copying, modification (e.g. in the context of error correction and plausibility checks), deletion and blocking of the data. The time, purpose and nature of the access must be logged, information which is identified clearly by the persons accessing the data stored on a compulsory basis in accordance with § 113b. Information connected with data usage as per § 113c(1) of the Draft Telecommunications Act is logged in compliance with the provisions concerning logging in the statutory instrument under § 110(2).

Re paragraph 2

Paragraph 2 stipulates that the protocol control information may not be used for purposes other than data protection control purposes.

Re paragraph 3

The provision relating to deletion in paragraph 3 complies with the example under § 112(4) sentence 6 of the Telecommunications Act.

Re § 113f of the Draft Telecommunications Act

According to § 113f of the Draft Telecommunications Act, a particularly high safety and quality standard must be ensured when implementing the obligations in accordance with §§ 113b to 113e of the Draft Telecommunications Act. The technical substantiation of the standard specified is to be entrusted to the Federal Network Agency as the supervisory authority (cf. Federal Constitutional Court Decisions 125, 260 <327>).

The regulation under § 113f of the Draft Telecommunications Act supplements the provision under § 109(6) of the Telecommunications Act.

Re paragraph 1

Sentence 1 obligates the providers of publicly available telecommunications services to ensure a particularly high standard of data security and quality when implementing the obligations under §§ 113b to 113e of the Draft Telecommunications Act.

Sentence 2 stipulates that the Federal Network Agency, with the involvement of the Federal Office for Information Technology Security and the Federal Data Protection and Freedom of Information Commissioner, shall draw up a catalogue of requirements in terms of technical arrangements and other measures designed to fulfil the obligations arising from §§ 113b to 113e of the Draft Telecommunications Act. Observance of the standards specified in sentence 1 is assumed if the party obligated fulfils the requirements laid down in the catalogue.

The catalogue is to contain the following requirements in particular:

– in relation to the deletion of the data in accordance with § 113b(8) of the Draft Telecommunications Act, in which connection provision shall be made for the fact that the data shall be deleted in such a way that it is impossible to recover the data, including back-up copies,

– in relation to guaranteeing the security of the data as per § 113d of the Draft Telecommunications Act,

– for logging in an audit-proof manner in accordance with § 113e of the Draft Telecommunications Act, and

– with regard to ensuring a particularly high standard of data quality as per § 113f(1) sentence 1 of the Draft Telecommunications Act, for example, through using automated error detection methods, plausibility checks and measures designed to ensure the accuracy of the times to be stored.

Re paragraph 2

Paragraph 2 stipulates that the Federal Network Agency shall review the requirements contained in the catalogue on an ongoing basis. In so doing, it will take account of the state of the art and expert discussions in order to determine whether the catalogue has to be amended. If there is a need for change, the catalogue must be adapted immediately with the involvement of the Federal Office for Information Technology Security and the Federal Data Protection and Freedom of Information Commissioner.

Re paragraph 3

With reference to provisions under § 109(6) sentences 2 and 3 of the Telecommunications Act, paragraph 3 determines that when drawing up the catalogue, the Federal Network Agency shall give producers, associations of public telecommunications network operators and associations of providers of publicly available telecommunications services the opportunity to comment and then publish the catalogue.

Pursuant to § 113f(3) of the Draft Telecommunications Act, in conjunction with § 109(7) of the Telecommunications Act, the Federal Network Agency shall decree that the parties obligated in accordance with § 113b of the Draft Telecommunications Act shall undergo a review by a qualified independent body or a competent national authority in which it is determined whether the requirements arising from § 113b(7) and (8), § 113c, § 113e(1) and § 113f(1) sentence 1 are satisfied. The obligated party shall forward a copy of the review report to the Federal Network Agency forthwith. The obligated party shall also bear the costs of this review.

Re § 113g of the Draft Telecommunications Act

The regulation under § 113g of the Draft Telecommunications Act supplements the provision in § 109(4) of the Telecommunications Act in relation to the parties obligated in accordance with § 113a(1) of the Draft Telecommunications Act and thereby transposes

the stipulations of the Federal Constitutional Court regarding a verifiable regular adaptation of the security measures (Federal Constitutional Court Decisions 125, 260 <326, 350 f.>).

Sentence 1 determines that the party obligated in accordance with § 113a(1) of the Draft Telecommunications Act shall also include in the security concept to be drawn up by the party obligated in accordance with § 109(4) of the Telecommunications Act which systems are operated in order to fulfil the stipulations under §§ 113b to 113e of the Draft Telecommunications Act, which dangers shall be assumed for these systems, and which technical arrangements or other measures designed to fulfil the obligations arising from §§ 113b to 113e of the Draft Telecommunications Act have been taken or are planned in order to counter these dangers. The term "Systems" includes facilities and organisational arrangements.

Sentence 2 contains requirements with respect to the submission and resubmission of the security concept: The security concept shall be presented to the Federal Network Agency for the first time immediately after initiation of storage in accordance with § 113b of the Draft Telecommunications Act and again every time an amendment is made. If no changes are made to the security concept, it shall suffice that the obligated party explains this to the Federal Network Agency at intervals of 2 years each time. Regular resubmission of the unaltered concept is not therefore necessary.

Re point 3 (§ 121(1) of the Draft Telecommunications Act)

The provision is designed to ensure a publicly transparent check involving the independent Data Protection Commissioner and thereby transpose a corresponding stipulation of the Federal Constitutional Court (Federal Constitutional Court Decisions 125, 260 <327>).

It is specified that the Federal Network Agency shall communicate in its progress report, which is presented to the Federal Government's legislative bodies every 2 years, the extent to which it has reviewed security concepts and the compliance thereof in accordance with § 113g of the Draft Telecommunications Act, the outcomes of these reviews, and whether and which complaints and further outcomes the Federal Data Protection and Freedom of Information Commissioner has communicated to the Federal Network Agency in this respect.

Re point 4 (§ 149 of the Draft Telecommunications Act)

Re letter a

Supplementation of the catalogue of administrative offences in paragraph 1 to include points 36 to 44 is designed to ensure fulfilment of the obligations arising from §§ 113b to 113e and § 113g of the Draft Telecommunications Act and hence, in particular, comprehensive and effective protection of the data to be stored.

Re letter b

The amendment to paragraph 2 takes into account the judgment of the Federal Constitutional Court, according to which the current legal system lacks a balanced system of sanctions which does not ascribe any less importance to data security infringements than to infringements of storage obligations (Federal Constitutional Court Decisions 125, 260 <351>). Paragraph 2 therefore makes provision for the fact that any violations of the obligations which arise with regard to the data to be stored in accordance with § 113b of the Draft Telecommunications Act may be consistently punishable by a fine of up to EUR 500 000. In the case of infringements of the obligation to log all instances of access to the stored data (§ 113e of the Draft Telecommunications Act), provision is made for a

fine of up to EUR 300 000 and, in the case of the incomplete or untimely submission in the security concept of the information listed in 113g of the Draft Telecommunications Act, for a fine of up to EUR 100 000.

Re point 5 (§ 150(13) of the Draft Telecommunications Act)

The new paragraph 13 sentence 1 stipulates that the storage obligation as per § 113b of the Draft Telecommunications Act must be satisfied no later than 18 months after the promulgation of this Act. Sentence 2 determines that the Federal Network Agency shall publish the catalogue of requirements to be drawn up in accordance with § 113f(1) of the Draft Telecommunications Act no later than 12 months after the promulgation of this Act.

In this way, account is taken of the fact that both the parties obligated in accordance with § 113b of the Draft Telecommunications Act and the other authorities involved – Federal Network Agency, Federal Office for Information Technology Security and the Federal Data Protection and Freedom of Information Commissioner – are not necessarily able to implement the stipulations under law in the short term. Instead, certain technical, organisational or other (preparatory) measures are required to this end. For this reason, it seems appropriate to allow the obligations to enter into force at different times. The provision is especially designed to establish the precondition whereby the catalogue of requirements to be drawn up by the Federal Network Agency in accordance with § 113f of the Draft Telecommunications Act can be published prior to the entry into force of the storage and associated obligations according to §§ 113b to 113e and 113g of the Draft Telecommunications Act.

Re Article 3 (Amendment of the Act implementing the Code of Criminal Procedure [German designation: EGStPO])

§ 12 of the Draft Act implementing the Code of Criminal Procedure lays down two transitional provisions. Since the storage obligation under § 150 of the Draft Telecommunications Act cannot be implemented with the entry into force of the Act, but shall only be satisfied within 18 months of promulgation, retrieval would not be possible for stored location data in the intervening period since the amended § 100g(1) no longer makes provision for such a retrieval. § 100g(2) can only take effect, however, if the data are actually stored.

In addition, provision must be made for a transitional provision for the statistical obligations envisaged in § 101b. This is tied in with the time envisaged in § 150(13) of the Draft Telecommunications Act from when the storage obligation as per § 113b of the aforementioned act must be satisfied at the latest. The new provisions shall apply to the year under review following this time. The previous provision in § 100g(4) of the Code of Criminal Procedure shall apply to the preceding years under review.

Re Article 4 (Amendment of the Court Allowances Act)

Re point 1 (Table of contents)

Appendix 3 to the Court Allowances Act is previously not mentioned in the Table of contents. The corresponding indication shall be inserted from now on.

Re point 2 (§ 6(1) of the Draft Court Allowances Act)

The reference in § 6(1) of the Court Allowances Act to § 4(5) sentence 1 point 5 sentence 2 of the Income Tax Act must be adapted on account of the amendment to the Income Tax Act by means of Article 1 point 2a of the Act amending and simplifying company taxation and travel expense tax laws of 20 February 2013 (Federal Law Gazette I p. 285). The reference is to be effected in keeping with the provision in § 6(1)

sentence 2 of the German Travel Expenses Act, which has been reworded by means of Article 3 of the Tax Act mentioned.

Re point 3 (§ 23(2) sentence 1 of the Draft Court Allowances Act)

The provision shall also apply in penalty proceedings before the administrative authority. Therefore, this authority should be expressly referred to as a "prosecuting authority" as is already the case under § 13(2) sentence 1 and paragraph 6 sentence 2 of the Court Allowances Act.

Re point 4 (Preliminary observation regarding Appendix 2)

This constitutes an editorial correction.

Re point 5 (Appendix 3)

The compensation schemes for information concerning traffic data or inventory data, the granting of which must draw on traffic data, are to be modified for those cases in which recourse to data retained on the basis of the storage obligation as per § 113b(2) to (4) of the Telecommunications Act is necessary. The principle that two pairs of eyes are better than one, as stipulated in this respect in § 113d sentence 2 point 5 of the Draft Telecommunications Act, shall result in increased personnel deployment. The compensation lump sums must therefore be raised in these cases.

In addition to the inclusion of the new points 202 and 401, the proposal is making provision for a new version of section 3 of Appendix 3 to the Court Allowances Act for reasons of clarity. In the new points 202, 301, 304, 307, 309, 311, 315 to 317, 319 and 401, a 20 % increase in flat rates is proposed as regards the inclusion of data stored in accordance with § 113b(2), (3) or (6) of the Telecommunications Act. In this connection, the amounts are rounded off to five whole euros (EUR 5) each time. Underlying the proposal is the assumption that in the case of the principle that two pairs of eyes are better than one, the total expenditure in relation to implementation by one individual shall increase (only) slightly since the second person will not have to input the data again but simply check and approve the entries.

The amount of compensation should also then be determined, all in all, by the increased flat rates if the principle that two pairs of eyes are better than one is only prescribed in relation to one part of the data accessed.

Re Article 5 (Amendment of the German Criminal Code)

Re point 1 (Table of contents)

This constitutes a subsequent editorial amendment regarding the inclusion of § 202d of the German Criminal Code (Article 3 point 2).

Re point 2 (§ 202d of the Draft German Criminal Code)

On account of its connection with §§ 202a to 202c of the German Criminal Code, the new criminal offence of receiving stolen data are to be located in Chapter 15 of the Special Part of the German Criminal Code (Violation of privacy). §§ 202a to 202c of the German Criminal Code safeguard formal data secrecy on the part of that party which, on account of its right to intellectual content, shall take a decision on the disclosure and transmission of the data (*Münchener Kommentar*/Graf, 2nd edition, § 202a, recital 2) and, thereby, on its interest in maintaining the right of ownership over information (*Leipziger Kommentar*/Hilgendorf, 12th edition, § 202a, recital 6), without presupposing a violation of privacy (cf. *Bundestag* document no. 10/5058, p. 28). The new elements of the offence which safeguard formal data secrecy against the continuation and consolidation of its

infringement which has already taken place as a result of the prior offence are tied in with this.

Re paragraph 1

According to this provision, a party shall be liable to prosecution when it makes available for itself, or to someone else, data which another party has acquired as a result of an unlawful act, when it relinquishes said data to another party, or when it disseminates the data or makes it available in another way, in order to make money for itself or a third party or to injure someone else.

The criminal offence only covers data which is not publicly available. In the process, the provision refers to the legal definition of data in § 202a(2) of the German Criminal Code (Data espionage). Data within the meaning of § 202d of the German Criminal Code thus only refers to that data which is stored or transmitted electronically or magnetically, or in another manner which is not immediately noticeable.

The exclusion of data which is available to the general public follows from the fact that in these instances, there is an absence of encroachment on formal data secrecy safeguarded by the provision. The fact that the perpetrator does not draw on the generally accessible source but takes advantage of the prior offence could not therefore justify culpability. Publicly available data are defined in § 10(5) sentence 2 of the Federal Data Protection Act with regard to automated retrieval procedures as data which anyone can use, either without or following a prior application, approval or payment of a fee. Particularly therefore, published works protected by copyright are also generally accessible if a fee has to be paid to use them. Corresponding works obtained by the prior perpetrator as a result of a copyright infringement shall not therefore be covered by the facts of the case.

The data must have been acquired by another party as a result of an unlawful act (§ 11(1) point 5 of the German Criminal Code). Consequently, all acts which bring a criminal law to fruition, irrespective of the guilt of the perpetrator or of the presence of a demand for prosecution, shall come into consideration as regards the prior offence of receiving stolen data, as is also the case with receiving stolen property (cf. Fischer, German Criminal Code, 62nd edition, § 259, recital 6). Prior offences may therefore comprise not just data espionage and phishing (§§ 202a, 202b of the German Criminal Code) but also, for example, theft (§ 242 of the German Criminal Code), fraud (§ 263 of the German Criminal Code), computer fraud (§ 263a of the German Criminal Code), coercion (§ 240 of the German Criminal Code) and the forgery of data intended to provide proof (§ 269 of the German Criminal Code) if, in a given case, they are also directed against the formal right of disposal on the part of the authorised individual and the perpetrator has acquired data as a result. Likewise, the acquisition of data in the course of preparations to counterfeit guaranteed payment cards (§ 152b(5), in conjunction with § 149(1) point 1 of the German Criminal Code; regarding so-called skimming, cf. Federal Court of Justice, decision of 29 January 2014 – 1st constitutional law 654/13) comes into consideration. Ultimately, the receipt of stolen data likewise comes into consideration as a prior offence in the same way, in principle, as criminal offences under the Federal Data Protection Act.

The prior offence must (also) be directed against the formal right of disposal on the part of the authorised individual. The authorised individual is that party who may dispose of the data (cf. *Leipziger Kommentar*/Hilgendorf, 12th edition, § 202a, recital 26), i.e. basically that party which has collected and stored the data or has instigated storage (cf. BayOLG [Bavarian Supreme Court], judgment of 14 June 1993, JR 1994, pp. 476, 477; *Münchener Kommentar*/Graf, 2nd edition, § 202a, recital 19). Ownership and possession of the data storage device are not decisive to this end. The entitlement shall be set apart from the concern under data protection law. The party concerned is the identified or identifiable natural person regarding whom the data contains particulars concerning personal or

material circumstances (§ 3(1) of the Federal Data Protection Act). The formal entitlement and the concern under data protection law may coincide.

In accordance with the legal position, as regards receiving stolen property (cf. Maurach/Schroeder/Maiwald, Criminal law, Special Part, 10th edition, § 39, recital 20), it is sufficient that the prior offence, irrespective of its systematic classification in terms of its practical implications, infringes the formal right of disposal on the part of the authorised individual. A prior offence directed against the formal right of disposal is especially lacking if the offence only contravenes public interests such as, for example, § 184d of the German Criminal Code (Distribution of pornographic performances by broadcasting, media services or telecommunications services). This shall also apply if the prior perpetrator has compiled data themselves and shall thereby be liable to prosecution in accordance with the Federal Data Protection Act (cf. § 44 thereof), since an encroachment on the formal right of disposal presupposes that the data were subject beforehand to the authority to dispose on the part of the authorised individual.

Data which is already available to the prior perpetrator and which they reproduces in violation of copyright constitutes data that has not been acquired as a result of an unlawful act, nor does the prior perpetrator obtain data as a result of an unlawful act if they merely commits a breach of contract, a disciplinary offence or an administrative offence. If, in a system that is used under authorisation, data are merely acquired in contravention of contractual access restrictions, this is insufficient to constitute a prior offence.

As follows from the wording "has acquired", the prior offence must already have been completed in accordance with the provision concerning the receipt of stolen property (§ 259 of the German Criminal Code) if the perpetrator makes data available for themselves, or to someone else, relinquishes said data to another party, or disseminates the data or makes it available in another way. It is not therefore *actus reus*, for example, if the prior offence is only committed as a result of transmitting the data to the party handling the stolen data (cf. regarding the legal position in the case of receiving stolen property, Federal Court of Justice decision of 24 October 2012 – 5th constitutional law 392/12).

The perpetrator must make available for themselves, or to someone else, the data acquired by the prior perpetrator, relinquish said data to another party, disseminate the data or make it available in another way. These acts constituting the offence are taken from § 202c(1) of the German Criminal Code (Acts preparatory to data espionage and phishing), meaning that the interpretation effected to this end in case-law and literature can be consulted. Adoption of the version of the "buying" element of the offence contained in § 259(1) of the German Criminal Code, as well as the "selling" element of the offence contained in § 202c thereof, as regards which it is disputed whether it can already be satisfied by means of the conclusion, under the law of obligations, of a (possibly void under civil law) purchase agreement (cf. Fischer, German Criminal Code, 61st edition, § 202c, recital 7), or whether the transfer of control over the data are also necessary to this end so that acquisition constitutes a subcategory of "procurement" (cf. *Leipziger Kommentar*/Hilgendorf, German Criminal Code, 12th edition, § 202c, recitals 22, 24) is dispensed with. Irrespective of the question of interpretation as regards § 202c of the German Criminal Code which is not yet settled by case-law, in any event, liability to punishment on account of receiving stolen data shall presuppose that the perpetrator obtains the data for themselves or a third party, i.e. actual authority over the data are acquired as a result of the act constituting the offence. Merely the contractually agreed acquisition of the data by the prior perpetrator, or its contractually agreed sale to a third party, shall still not result in a continuation or consolidation of the infringement of formal data secrecy and does not thereby exceed the threshold of culpability.

As is the case with receiving stolen property, mutually agreed collaboration between the perpetrator and prior perpetrator is necessary. In consultation with the prior perpetrator, the perpetrator must avail themselves of the opportunity established by the former, as a

result of their unlawful act, to be able to access the data. Liability to punishment on account of receiving stolen data are excluded if the perpetrator does indeed have knowledge of the prior offence but does not use the prior perpetrator as the source of the data, accessing it in another way instead. It is thereby not sufficient that the perpetrator only cooperates with another party who has acquired the data not as a result of their own unlawful act, but only as a result of the unlawful act committed by a third party (e.g. by violating official secrets, § 353b of the German Criminal Code). Direct contact between the perpetrator and prior perpetrator is not necessary, meaning that liability to punishment is not excluded on account of using middlemen.

Liability to punishment is excluded if the authorised individual injured as a result of the prior offence buys back the data stolen from them (cf. *Münchener Kommentar*/Maier, 2nd edition, § 259, recital 60). Perpetration by the person concerned simply under data protection law (just as in the case of § 202a of the German Criminal Code, cf. *Münchener Kommentar*/Graf, 2nd edition, § 202a, recital 19) does come into consideration, however.

The perpetrator must act wilfully and knowingly. Their intent must especially cover the circumstance whereby the data has been acquired by someone else as a result of an unlawful act. As is the case with receiving stolen property, for this it is necessary that the perpetrator approves (eventually) the completion of the offence which is recognised as feasible and not entirely far-fetched or at least reconciles themselves to it for the sake of the desired goal (Federal Court of Justice, decision of 23 November 1999 – 4th constitutional law 491/99, wistra 2000, pp. 177 f.). By itself, awareness of the fact that the data originates from some unlawful act or other is not sufficient for justifying the intent (cf. regarding the receipt of stolen property, the Federal Court of Justice, decision of 13 November 2012 – 3rd constitutional law 364/12, NStZ-RR [*Neue Zeitschrift für Strafrecht, Rechtsprechungsreport*] 2013, p. 79). The precise details of the prior offence, i.e. its nature, the circumstances under which it was committed or the person responsible for committing it do not have to be known (*Beck'sche Online-Kommentar*, German Criminal Code/Ruhmannseder German Criminal Code, § 259, recital 40). The perpetrator shall also include in their intent the fact that the data in question is not publicly available. Intent must be a given at the time of the act constituting the offence (cf. Schönke/Schröder/Stree/Hecker, German Criminal Code, § 259, recital 39). Should the perpetrator subsequently learn of the illegal origin of the data, they shall only fulfil the elements of the offence if, following this, they carry out criminal actions such as the dissemination of the incriminating evidence (Schönke/Schröder/Stree/Hecker, German Criminal Code, 29th edition, § 259, recital 41).

The perpetrator must act with the intent of making money for themselves or a third party or injuring someone else. This corresponds to the provision under § 44(1) of the Federal Data Protection Act, meaning that the interpretation developed to this end by case-law and literature can be consulted. According to this, an (outside) intent to profit exists if, according to the notion of the perpetrator, the deed is directed at the acquisition of a pecuniary advantage for the perpetrator themselves or a third party, in which connection *dolus directus* of the first degree is required with regard to enrichment (*Beck'sche Online-Kommentar* DatenSR/Holländer, Federal Data Protection Act, § 44, recital 9). In contrast to § 263 of the German Criminal Code, this pecuniary advantage may be unlawful in nature, but does not have to be (cf. Simitis, Federal Data Protection Act, § 3, recital 6). The intent to cause injury exists with every drawback imposed on another individual, including intangible ones, which is the intention of the perpetrator (e.g. the trade in data for the purpose of public exposure on the internet), in which connection it must depend on them injuring another person as a result of the completion of the offence (*Beck'sche Online-Kommentar* DatenSR/Holländer, Federal Data Protection Act, § 44, recital 11).

The act shall be threatened with a prison sentence of up to 3 years or a fine. This range of sentences corresponds to the threat of punishment under § 202a(1) of the German Criminal Code, which safeguards formal data secrecy just like the receipt of stolen data.

Re paragraph 2

The punishment may not be more severe than that threatened in relation to the prior offence. The regulation corresponds to the provision under § 258(3) of the German Criminal Code (Obstruction of justice) and takes account of the fact that offences which carry a lesser threat of punishment come into consideration as prior offences, such as phishing, for example, as per § 202b of the German Criminal Code. The maintenance and consolidation of the infringement of formal data secrecy which follows as a result of receiving stolen data should not be punished more severely than the infringement of this object of legal protection as a result of the prior offence.

Re paragraph 3

§ 202d(3) of the German Criminal Code makes provision for an exclusion from the category for actions which exclusively serve the purpose of fulfilling lawful, official or professional obligations. This particularly includes those activities of officials by means of which data are to be supplied exclusively for utilisation in a taxation procedure, criminal proceedings or non-compliance procedures.

The provision corresponds to the exclusion from the category provided for in § 184b(5) of the German Criminal Code (Possession of child pornography). The provision ensures that data may be used in particular for the purposes of investigations and for journalistic activities.

The exclusion from the category shall apply to officials (§ 11(2) point 2 of the German Criminal Code) and also to persons outside the authority who are commissioned by an official in a specific given case on the basis of an order under private law. These persons make data available to the officials which then aid them in the fulfilment of their official obligations. This applies accordingly to the enlisting of authorised representatives as regards the fulfilment of professional obligations.

As is the case under § 184b(5) of the German Criminal Code, professional obligations also cover in particular journalistic activities in preparation for a specific publication (cf. *Münchener Kommentar*/Hörnle, 12th edition, § 184b, recital 41). It is to be ensured by means of the exclusivity criterion in accordance with the provision under § 184b(5) of the German Criminal Code that the fulfilment of specific tasks is the sole reason for using the data (cf. *Bundestag* document no. 12/4883, p. 8 f.).

§ 202d(3) sentence 2 of the German Criminal Code constitutes a subcategory of § 202d(3) sentence 1 of the German Criminal Code. It clarifies, on the one hand, the fact that the acquisition, in particular, of data which is relevant according to tax law does not come under the scope of receiving stolen data. On the other hand, it is made clear that in accordance with the provision under § 184b(5) of the German Criminal Code, journalistic activities in particular do come under exclusion from the category. To this end, it does not matter whether these activities have been imposed at third hand, meaning that the journalist's voluntary decision within the framework of their professional duties is also covered (cf. Schönke/Schröder/Eisele, German Criminal Code, 29th edition, § 184b, recital 16). The provision is based on § 353b(3a) of the German Criminal Code, meaning that reference can be made to the principles of interpretation developed to this end. The persons mentioned in § 53(1) sentence 1 point 5 of the Code of Criminal Procedure include those who make, or have made, a professional contribution to the preparation, production or dissemination of printed matter, radio broadcasts, film reports or to the information and communication services which assist in providing instructions or shaping opinion.

Re point 3

The relative requirement to make a criminal complaint provided for in § 205(1) sentence 2 of the Draft German Criminal Code (Demand for prosecution) shall also apply to the criminal offence of receiving stolen data. The act shall only be prosecuted on request unless the criminal prosecution authority officially deems intervention to be necessary on account of special public interest in the prosecution.

Re Article 6 (Restrictions on fundamental rights)

By means of this provision, the citation requirement under Article 19(1) sentence 2 of the Basic Law is satisfied.

Re Article 7 (Entry into force)

This provision regulates the entry into force of this Act.