Draft Law

of the Federal Government

Draft Law on the Introduction of IP Address Storage and Further Development of Data Collection Powers in Criminal Proceedings

A. Problem and objective

Criminal offences often have digital components, for example, in the communication of suspects via messenger services, the distribution of child pornography, criminal trading platforms offering narcotics or Cybercrime-as-a-Service (CaaS), and seemingly legitimate online shops selling goods that do not actually exist (fake shops). The perpetrators leave digital traces, for example the Internet protocol address (IP address) they use. These traces are often fleeting, as internet service providers only store IP addresses for a few days, if at all. A query from law enforcement authorities and other authorised agencies to the Internet access service providers is therefore only successful if the requested data is still stored. Furthermore, following a ruling by the Federal Court of Justice, cell site data retrieval is no longer permitted in cases involving serious criminal offences.

The aim of the draft is to improve the likelihood of success for queries made by law enforcement agencies and other authorised bodies, and to enable law enforcement agencies to carry out cell site queries to the same extent as before the Federal Court of Justice’s ruling.

B. Solution; benefits

Firstly, a requirement to retain IP addresses will be introduced to enable law enforcement agencies and other authorised bodies to reliably identify a subscriber on the basis of an IP address. The authorities can thus use a tool that allows them to follow the often only, but almost always most efficient, investigative approach. Secondly, in the field of law enforcement and security, the Federal Police will be granted the power to issue preservation orders for traffic data. This allows these authorities to arrange for traffic data to be secured if and as long as the legal or factual requirements for data collection have not yet been met. Thirdly, law enforcement authorities will once again be permitted to carry out cell site analysis in cases involving offences of significant importance, in particular those under § 100a(2) of the Code of Criminal Procedure (Strafprozessordnung).

C. Alternatives

None.

D. Budget expenditure excluding compliance costs

The new regulations will result in the following requirements for the federal budget:

In the budget of the Federal Ministry of the Interior, Section 06, additional personnel and material costs are incurred by the Federal Office for the Protection of the Constitution. The

necessary technical adjustments are expected to incur around EUR 254 000 in one-off material costs in the financial year 2027. Additional material costs of EUR 177 000 are expected for day-to-day operations from 2027 onwards. According to current estimates, the necessary technical adjustments entail an additional requirement of four (plan) posts (1 A14, 1 A12, 1 A11, 1 E9a). The additional personnel costs amount to EUR 372 000.

In the budget of the Federal Ministry of Justice and Consumer Protection, Section 07, the Federal Court of Justice and the Federal Public Prosecutor at the Federal Court of Justice will incur minimal additional administrative costs for preservation orders from 2027 onwards; according to current forecasts, these will be well below 1 000 euro per year.

In the budget of the Federal Ministry of Finance, Section 08, no additional personnel or material costs are expected to be incurred by the authorities of the customs administration.

Additional expenditure set out above, as well as any other additional expenditure, is to be offset in terms of both funding and staffing within the relevant budget section.

In the budget of the Federal Ministry for Economic Affairs and Energy, Section 09, the Federal Network Agency (Bundesnetzagentur) has an estimated additional staff requirement of 26 posts from the financial year 2027 for the technical tasks (1 A16, 1 A15, 1 A14, 1 A13gZ, 3 A13g, 5 A12, 5 A11, 1 A10, 1 A9mZ, 2 A9m, 3 A8, 1 A7, 1 A6m) with annual individual staff costs totalling EUR 2.376 million, unit costs of EUR 891 000 and overhead costs of EUR 960 000. The additional horizontal tasks require a further 7.8 posts (respectively 0.3 A16, A15, A14 and A13gZ, 0.9 A13g, 1.5 A12 and A11, 0.3 A10 and A9mZ, 0.6 A9m, 0.9 A8 and 0.3 A7 and A6m). Additional personnel and material costs for cross-cutting tasks are included in overheads. In addition, there will be annual running material costs of EUR 5 000 from the financial year 2027 and one-off material costs of EUR 25 000 in 2027 for the extension of an existing laboratory facility.

Additional revenue is expected in the budget of the Federal Ministry for Economic Affairs and Energy as a result of additional fine proceedings. The amount of revenue depends on the number of proceedings and the seriousness of the infringements, and cannot be predicted.

Additional requirements in terms of posts are to be offset in Section 09. The additional financial requirements are to be offset in the relevant sections in terms of funding and staffing.

The regional governments are expected to see a shortfall in their budgets totalling €1.429 million. This is not expected to have any impact on local authority budgets.

E. Compliance costs

E.1 Compliance costs for citizens

None.

E.2 Compliance costs for businesses

None.

E.3 Compliance costs for the authorities

None.

F. Other costs

The regulations on IP address storage and the introduction of a preservation order for traffic data concern the judicial core area. It can be assumed that the implications will be largely cost-neutral for both the federal government and the Länder. There are additional costs for the economy. However, effects from this on individual prices and the general price level, in particular the consumer price level for telecommunications services, are not anticipated.

Draft Law of the Federal Government

Draft Law on the Introduction of IP Address Storage and Further Development of Data Collection Powers in Criminal Proceedings[1]

of ...

The Federal Parliament has adopted the following Act:

Artikel 1

Amendment to the Criminal Procedure Code

the Criminal Procedure Regulation in the version as published on 7 April 1987 (Federal Law Gazette I p. 1074, 1319), last amended by Article 7 of the Law of 20 March 2026 (Federal Law Gazette 2026 I No. 95), is amended as follows:

1. The table of contents is amended as follows:

   a) The wording for § 100j is replaced by the following wording:

   ‘§ 100j Collection of inventory data’.

   b) The wording for § 101a is replaced by the following wording:

   ‘§ 101a Procedural rules for the collection of traffic, use and inventory data’.

2. § 100g is replaced by the following § 100g:

‘§ 100g

Traffic data collection

(1) Traffic data relating to the suspect, as defined in § 3(70) of the Telecommunications Act, with the exception of data stored pursuant to § 177(1) of the Telecommunications Act, may be collected from any person who provides or contributes to the provision of publicly available telecommunications services,

1. where there are specific facts giving rise to a suspicion that a person has committed, as the perpetrator or an accomplice, a criminal offence of significant importance even in the individual case, in particular an offence referred to in § 100a(2), or, in cases where an attempt is a criminal offence, has attempted to commit such an offence or has made preparations for it through a criminal offence,

2. insofar as the collection of traffic data is necessary for investigation of the facts or for determination of the whereabouts of the accused and

[1] Notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17/9/2015, p. 1).

3. provided that the collection of traffic data is proportionate to the importance of the matter.

Sentence 1 applies mutatis mutandis to the collection of traffic data relating to persons in respect of whom there are grounds for believing that they receive or transmit messages intended for or originating from the accused, or that the accused uses their connection or information technology system. Sentences 1 and 2 shall apply mutatis mutandis to the collection of traffic data pursuant to § 2a(1) of the BDBOS Act from the Federal Agency for Digital Radio of authorities and organisations with security responsibilities.

(2) Where there is no suspicion of a criminal offence of significant importance, even in the specific case, the collection of traffic data is permitted, subject to the other conditions set out in paragraph 1, provided that the following requirements are met:

1. specific facts give rise to a suspicion that a person has committed a criminal offence as a perpetrator or an accomplice using telecommunications, in cases where an attempt to commit such an offence is a criminal offence, or has attempted to commit such an offence, or has made preparations for such an offence, and

2. notwithstanding paragraph 1, first sentence, point 2, investigating the facts in any other way would be futile or significantly more difficult; an inquiry to determine the whereabouts of the accused is not permitted.

(3) Location data within the meaning of § 3(56) of the Telecommunications Act may be collected under the conditions set out in paragraph 1, subject to the proviso that, by way of derogation from point 2 of the first sentence of paragraph 1, collection is permitted only if investigation of the facts or determination of the whereabouts of the accused person would otherwise be futile or significantly more difficult.

(4) The collection of all traffic data generated in a radio cell (radio cell query) shall be permitted under the conditions laid down in paragraph 3.

(5) By way of derogation from paragraphs 1 and 2, the law enforcement authority may, in the case of a number-independent interpersonal communications service, if it is already aware of the content of the use of the service, collect the following for the purpose of identifying the accused:

1. the public Internet protocol address stored for him,

2. the date and exact time (to the second) when the public IP address was recorded, specifying the relevant time zone, and

3. the port numbers associated with the Internet Protocol address and other traffic data, insofar as these are necessary for identification of the accused on the basis of an Internet Protocol address assigned at a certain point in time.

Paragraph 1(2) shall apply accordingly.

(6) If traffic data are not collected from the obligated party in accordance with paragraph 1 sentence 1 or 3, their admissibility shall be determined after completion of the communication process in accordance with the general rules.

(7) For the purposes of any collection pursuant to paragraphs 1 to 4, obliged entities may be ordered to preserve traffic data of data subjects without undue delay (preservation order);

1. where there are sufficient factual grounds to suggest that a criminal offence has been committed which would justify the initiation of proceedings in accordance with paragraphs 1 to 4,

2. if the person concerned has a personal or geographical connection to the offence referred to in point 1 and

3. to the extent that the data may be relevant for the purposes referred to in paragraphs 1 to 4.

The data secured in accordance with the first sentence shall be collected in accordance with paragraphs 1 to 4.’

3. § 100j and § 100k are replaced by the following § 100j and § 100k:

‘§ 100j

Collection of subscriber data

(1) ‘Insofar as this is necessary for researching the facts or for determining the whereabouts of a suspect, information may be requested

1. on subscriber data pursuant to § 3(6) of the Telecommunications Act and on data collected pursuant to § 172(1) of the Telecommunications Act from persons providing or participating in publicly available telecommunications services, and

2. on subscriber data in accordance with § 2(2)(2) of the Telecommunications Digital Services Data Protection Act at the premises of the provider of digital services.

(2) The information referred to in paragraph 1 may also be requested on the basis of an Internet Protocol address assigned at a specific point in time.

(3) Where the request for information under paragraph 1(1) relates to data used to protect access to terminal equipment or to storage devices used within such terminal equipment or in a separate location (§ 174(1), second sentence, of the Telecommunications Act), such information may only be requested if the legal requirements for the use of the data are met. If the request for information under paragraph 1(2) relates to passwords or other data collected as inventory data, which are used to protect access to end devices or to storage devices used within those end devices or physically separate from them (§ 23 of the Telecommunications and Digital Services Data Protection Act), information may only be requested if the legal requirements for its use in the prosecution of a particularly serious criminal offence under § 100b(2)(1)(a), (c), (e), (f), (g), (h) or (m), (3)(b) (first alternative) or (5), (5a), (5b), (6), (9) or (10) are met.

§ 100k

Collection of usage data for digital services

(1) Usage data relating to the accused, as defined in § 2(2)(3) of the Telecommunications and Digital Services Data Protection Act, may be collected from the provider of digital services subject to the conditions set out in § 100g(1), first sentence. § 100g(1) Sentence 2 applies accordingly.

(2) § 100g(2) shall apply mutatis mutandis to the collection of usage data from the obliged entity pursuant to paragraph 1, with the proviso that collection is permissible in case of suspicion of a criminal offence committed by means of a digital service.

(3) Location data may be collected from the data subject referred to in paragraph 1 in accordance with the conditions set out in § 100g(3).

(4) Usage data for the purpose of identifying the accused may be collected from the party subject to the obligation under paragraph 1, subject to the conditions set out in § 100g(5).

(5) The collection of usage data pursuant to paragraphs 1 to 3 shall only be allowed where facts justify the assumption that the data subject is using the obliged entity's digital service.

(6) If the collection of usage data relating to a digital service is not carried out by the party subject to the obligation under paragraph 1, its lawfulness after the communication process has been completed shall be determined in accordance with the general provisions.'

4. § 101a is replaced by the following § 101a:

'§ 101a

Procedural arrangements for the collection of traffic, use and inventory data

(1) § 100e(1), (3) (1) and (2) (1) to (5), and (5) (1) and (2) shall apply mutatis mutandis to the following proceedings:

1. when collecting traffic data in accordance with Section 100g(1) to (4), provided that

   d) the operative part of the decision must, in accordance with § 100e(3), second sentence, also clearly specify the data to be transferred and the period for which it is to be transferred, and

   e) in the case of base station queries pursuant to § 100g(4), a spatially and temporally narrowly defined and sufficiently specific description of the telecommunications is sufficient in the operative part of the decision, notwithstanding § 100e(3), second sentence, point 5,

2. when collecting usage data in accordance with § 100k(1) to (3), provided that

   d) in the operative part, notwithstanding § 100e(3), second sentence, point 5, a unique identifier for the data subject's user account must be provided where possible; otherwise, the digital service to which the request for information relates must be described as precisely as possible; and

   e) the decision formula shall also clearly indicate the data to be transmitted and the period for which they are to be transmitted;

3. in the case of a preservation order pursuant to § 100g(7), with the proviso that:

   d) notwithstanding § 100e(1), first to third sentences, the measure may be ordered by the public prosecutor's office for a maximum of three months, or,

in cases of imminent danger, by its investigating officers (§ 152 of the Courts Constitution Act), and the measure may be extended by the court for a maximum of three months only upon application by the public prosecutor's office,

e) the operative part of the decision must, in accordance with § 100e(3), second sentence, clearly specify the data to be preserved and the period for which it is to be preserved, and

f) when securing data from a radio cell pursuant to § 100g(3), in the operative part of the decision, by way of derogation from § 100e(3), second sentence, point 5, a spatially and temporally narrowly defined and sufficiently specific description of the telecommunications is sufficient.

§ 100e(1), first to third sentences, and (3), first and second sentences, points 1 to 4, shall apply mutatis mutandis with regard to the procedures for the collection of inventory data pursuant to § 100j(3), with the proviso that:

1. instead of § 100e(1), second sentence, the court decision must be obtained without delay and

2. in the operative part of the decision pursuant to § 100e(3), second sentence, point 3, the duration and end date of the measure need not be specified.

The second sentence shall not apply to requests for information pursuant to the first sentence of § 100j(3) if the data subject already has or must have knowledge of the request for information or if use of the data is already authorised by a court decision.

(2) Where a measure is ordered or extended pursuant to § 100g(1) to (4) or (7), § 100g(3) or § 100k(1) to (3), the statement of reasons shall set out, in particular on a case-by-case basis, the essential considerations relating to the necessity and appropriateness of the measure, including with regard to the scope of the data to be collected and the period for which they are to be collected.

(3) Personal data collected through measures taken pursuant to § 100g(1) to (4), § 100j(3) or § 100k(1) to (3) must be marked accordingly and analysed without delay. Once the information has been forwarded to another body, that body must continue to maintain the identification. § 101(8) applies mutatis mutandis to the erasure of personal data.

(4) The parties involved in the telecommunications network concerned and the users of the digital service concerned must be notified of any data collection in accordance with § 100g(1) to (5), § 100j(2) and (3), and § 100k(1) to (4). § 101(4), sentences 2 to 5, and paragraphs 5 to 7 shall apply mutatis mutandis.

(5) With regard to the duty to cooperate on the part of persons subject to the obligations under § 100g, 100j and 100k, § 100a(4) applies mutatis mutandis.'

5. § 101b is amended as follows:

a) In the first sentence of paragraph 1, the words 'paragraph 1 and 2' is deleted.

b) Paragraph (5) is amended as follows:

a%6) In point 1, in the indication before (a), the words '§ 100g(1), (2) and (3)' are replaced by the words '§ 100g(1), (2), (3), (4) and (7)'.

b%6) Point 2 shall be amended to read as follows:

a%7%7) After subparagraph c, the following subparagraphs d and e are inserted:

‘d) the number of orders made under § 100g(4);

a) the number of orders referred to in § 100g(7);’.

b%7%7) The previous subparagraphs d and e are renamed f and g.

c) In paragraph 6, in the information before point 1, the words ‘according to paragraphs 1 and 2’ are replaced by the words ‘according to paragraphs 1, 2, and 3’.

6. § 160a(5) is replaced by the following:

‘(5) § 97 and 100d(5) remain unaffected.'

Artikel 2

Amendment of the Act implementing the Code of Criminal Procedure

The Act implementing the Code of Criminal Procedure, in the corrected version published in Federal Law Gazette, Part III, No 312-1, as last amended by Article 4 of the Act of 8 December 2025 (Federal Law Gazette 2025 I No. 319) is amended as follows:

§ 12 is replaced by the following § 12:

‘Sec. 12

Transitional provision to the Law on the Introduction of IP Address Storage and Further Development of Data Collection Powers in Criminal Proceedings

overviews pursuant to § 101b(5) and (6) of the Code of Criminal Procedure in the version dated... [insert: date of entry into force in accordance with Article 13 of this Act] shall apply for the first time to the... [insert: date of entry into force in accordance with Article 13 of this Law] the following reporting year. For previous reporting years, § 101b(5) and (6) of the Code of Criminal Procedure in the version up to and including... [insert: date of the day before the entry into force pursuant to Article 13 of this Act].’

Artikel 3

Amendment to the Act on the Implementation and Enforcement of the Electronic Evidence Act

The Act on the Implementation and Enforcement of the Electronic Evidence Act of 10 March 2026 (Federal Law Gazette 2026 I No 64) is amended as follows:

1. In the table of contents, the following is inserted after the reference to § 10:

'§ 10a: Procedure for European Preservation Orders'.

2. After § 10, the following § 10a is inserted:

‘§ 10a

Procedures relating to European Preservation Orders

(1) The jurisdiction of the courts and public prosecutor’s offices to issue European preservation orders for the purpose of obtaining subscriber data or data requested for the sole purpose of identifying the user pursuant to Article 4(3)(a), of Regulation (EU) 2023/1543, as amended on 12 July 2023, and for the transmission of the corresponding certificate, shall be governed by Section 8 of Book I of the Code of Criminal Procedure.

(2) In a justified emergency situation as referred to in Article 4(5) of Regulation (EU) 2023/1543 in the version of 12 July 2023, the following entities shall be competent to issue European Preservation Orders and transmit the accompanying certificate in accordance with Article 4(3)(b), of Regulation (EU) 2023/1543 in the version of 12 July 2023, under the conditions set out therein:

1. the investigators of the public prosecutor's office (§ 152 of the Act to the Courts Constitution Act),

2. the tax authorities in the cases referred to in § 399(1) and § 386(2) of the Fiscal Code,

3. the customs authorities in the cases referred to in § 14a and § 14b of the Act to Combat Undeclared Work and Unlawful Employment.

(3) In cases referred to in paragraph 2, the issuing authorities shall transmit the European Preservation Order to the Public Prosecutor’s Office for ex-post validation within the period referred to in the second sentence of Article 4(5) of Regulation (EU) 2023/1543, as amended on 12 July 2023. Transmission of the certificate by the issuing authority and the decision on its validation by the public prosecutor’s office must be recorded in the case file.

(4) The public prosecutor's office conducting the investigation shall have local jurisdiction with regard to validation. If, under national law, the tax authorities or customs authorities conduct the investigation themselves, the public prosecutor's office at the regional court in whose district the issuing authority is located shall have jurisdiction with regard to validation. The federal states may lay down different rules regarding local jurisdiction.

(5) 'The public prosecutors’ offices and the juvenile court judge, in their capacity as enforcement officers, are responsible for issuing European preservation orders for the purposes of the enforcement of criminal sentences within the meaning of Article 4(3)(a) of Regulation (EU) 2023/1543, as amended on 12 July 2023, and for transmitting the relevant certificate.'

Artikel 4

Amendment to the Judicial Remuneration and Compensation Act

The Act on Remuneration and Compensation in the Judicial System of 5 May 2004 (Federal Law Gazette I pp. 718, 776), last amended by Article 13 of the Act of 8 December 2025 (Federal Law Gazette 2025 I No. 318), is amended as follows:

1. In § 23(1), the word ‘telecommunications’ is inserted after the word ‘or preservation orders’.

2. Annex 3 is amended as follows:

a) Paragraph 2 of the Preliminary Remarks is replaced by the following paragraph 2:

‘2. For services requested and invoiced by the law enforcement authorities through a central contact point of the Federal Prosecutor General, the Federal Criminal Police (Bundeskriminalamt) Office, the Federal Police or the Customs Criminal Police Office or through corresponding contact points responsible for one or more countries, the compensation amounts shall be reduced by 20 per cent in accordance with points 100, 101, 200 to 202, 300 to 308 and sections 4 to 6.’

b) Point 201 is replaced by the following Point 201:

No.	Activity	Height
„201	Information regarding inventory data, the provision of which requires the use of traffic data: for up to three identifiers requested simultaneously in the same process, which form the basis for the provision of the information..... If more than three identifiers are requested, the flat-rate allowance will be granted again for up to three additional identifiers in each instance. Identifier is also an IP address.	€15.00’.

c) The heading of Section 3 is replaced by the following heading:

‘Section 3

Information relating to traffic data without a prior preservation order’.

d) The following Preliminary remark 3 is inserted after the heading of Section 3:

‘*Preliminary remark 3:*

Line costs shall only be compensated if the line concerned has been used to transmit traffic data at least once. The compensation shall be paid for the entire transmission period.’

e) The heading of Section 4 is replaced by the following heading:

‘Section 4

Other information without previous preservation order’.

f) The following Sections 5 and 6 are inserted after Section 402:

No.	Activity	Height
	‘Section 5 ***Backup of data***	

Backing up traffic data: for each identifier on which the backup instruction is based ..... The securing of location data relating to the identifier is included.	€25.00
Backup of traffic data for a radio cell designated by the law enforcement authority	€40.00
Backup of traffic data for more than one mobile phone cell specified by the law enforcement agency: For each additional radio cell, the flat rate 501 shall be increased by:	€5.00
Backup of traffic data in cases where only the location and time period is known: Backup is performed for a specific location identified by an address	€75.00
Backup is carried out for one area: The compensation referred to in point 503 shall be:	€190.00
Backup applies to a specific section of the route: The compensation referred to in point 503 shall be, for each 10-kilometre period commenced:	€65.00
Backing up data relating to the last location of a mobile phone known to the network…	€85.00
Extension of retention period for data backed up in each of the cases referred to in points 500, 501 and 503 to 506	€25.00
Section 6 ***Disclosure of information following a prior preservation order***	
Information regarding data provided a preservation order subject to compensation under Section 5 has been issued: € per request for information	€20.00’.

Artikel 5

Amendment of the Administrative Offences Act

The Administrative Offences Act in the version published on 19 February 1987 (Federal Law Gazette I p. 602), as last amended by Article 21 of the Act of 22 December 2025 (Federal Law Gazette 2025 I No. 349), is amended as follows:

In § 46(4a), the words ‘§ 100j(1), first sentence, point 2’ are replaced by the words ‘§ 100j(1), point 2’.

Artikel 6

Amendment to the Telecommunications Act

The Telecommunications Act of 23 June 2021 (Federal Law Gazette I § 1858), as last amended by … [Article 2 of the draft Act implementing a European Union regulation on the exchange of data relating to short-term rentals and on the enforcement of European Union prohibitions on discrimination, Bundestag Paper 21/3484], is amended as follows:

1. In the table of contents, the entry for § 175 to § 181 is replaced by the following entry:

'§ 175 Disclosure of traffic data to law enforcement and security authorities

2. § 175 to § 181 are replaced by the following § 175 to § 177:

'§ 175

Authorisation to process traffic data for the purpose of providing information to law enforcement and security authorities

(1) Any person who provides or participates in publicly available telecommunications services may process traffic data in accordance with this provision in order to fulfil information obligations vis-à-vis the bodies referred to in paragraph 3. At the request of the Federal Network Agency, the person who stores this data must be informed immediately. § 32 of the statutory instrument issued pursuant to § 170(5) shall apply mutatis mutandis to the provision of information referred to in the first sentence.

(2) The information referred to in the first sentence of paragraph 1 may only be provided in accordance with the following paragraphs and in so far as there is a request for information from a body referred to in paragraph 3 containing the statutory provision allowing the body requesting information to collect traffic data. The responsibility for ensuring that the request for information is lawful lies with the authorities making the request.

(3) The information referred to in the first sentence of paragraph 1 may only be provided to

1. the authorities responsible for the prosecution of criminal offences, subject to the conditions set out in § 100g of the Code of Criminal Procedure,

2. the law enforcement authorities of the federal states, insofar as this is necessary in individual cases to avert a specific threat to a legal interest of at least considerable importance or to avert a specific threat to public safety,

3. the Federal Police, in accordance with the provisions of § 25(1) of the Federal Police Act,

4. the Federal Criminal Police Office under the conditions laid down in § 52(1) of the Federal Criminal Police Office Act (Bundeskriminalamtgesetz),

5. the Customs Criminal Investigation Office (Zollkriminalamt) under the conditions laid down in § 77(1) of the Customs Investigation Service Act (Zollfahndungsdienstgesetz),

6. the Federal Office for the Protection of the Constitution under the conditions laid down in § 8a(1), first sentence, point 4 of the Federal Constitutional Protection Act,

7. the constitutional protection authorities of the federal states, insofar as this is necessary on the basis of factual indications in individual cases in order to clarify certain aspirations or activities in accordance with

   d) § 3(1) of the Federal Constitutional Protection Act, or

e) a monitoring mandate conferred on the state authority by state law for the purpose of safeguarding the constitutional order (§ 1(1) of the Federal Act on the Protection of the Constitution), in particular to protect the constitutional order against the aims and activities of organised crime,

8. the Military Counter-Intelligence Service in accordance with the conditions set out in § 20(1), first sentence, point 5 of the MAD Act, and

9. the Federal Intelligence Service in accordance with the provisions of § 3 of the Federal Intelligence Service Act in conjunction with § 8a(1), first sentence, point 4 of the Federal Act on the Protection of the Constitution.

(1) § 174(6) sentence 2 and § 174(7) shall apply accordingly.

§ 2

Authorisation to process traffic data for the purpose of complying with preservation orders

(1) Any person who provides or contributes to the provision of publicly available telecommunications services may process traffic data to the extent necessary to fulfil

1. a preservation order pursuant to § 100g(7) of the Code of Criminal Procedure;

2. a preservation order pursuant to § 10b(1) or § 52(3) of the Federal Criminal Police Office Act , or

3. a preservation order pursuant to § 25a(1) of the Federal Police Act.

Traffic data secured solely on the basis of a preservation order in accordance with the first sentence may only be used for the specific purpose for which it was secured and may only be disclosed in accordance with the conditions set out in § 175. At the request of the Federal Network Agency, the person who stores this data must be informed immediately.

(2) Persons subject to a preservation order under paragraph 1, first sentence, must ensure that the traffic data preserved under paragraph 1

1. are protected against unauthorised access and use by means of state-of-the-art technical and organisational measures,

2. are stored in a manner that is technically and effectively separated from all other data held by the data controller relating to subscribers, using a secure and reliable data processing system,

3. are stored in such a way that they can be transmitted immediately to an ordering authority, provided that the latter requests such transmission on the basis of a statutory provision, and

4. shall be deleted immediately and irreversibly in accordance with the state of the art:

d) insofar as they are transmitted to the issuing authority in response to a request for information under paragraph 1, second sentence, following such transmission,

e) otherwise, after the expiry of the period specified in the preservation order.

(3) Persons subject to a preservation order under paragraph 1, first sentence, must maintain confidentiality regarding the existence of such an order, any related request for information, and any data transfer carried out on that basis, both towards the data subjects and third parties.

(4) The statutory instrument issued pursuant to § 170(5) may contain provisions setting out details of the obligations under paragraphs 2 and 3, as well as provisions governing the transmission of traffic data secured pursuant to preservation orders under paragraph 1, first sentence. Technical details for the implementation of these obligations shall be laid down in the technical guidelines pursuant to § 170(6). Providers of publicly available telecommunications services shall notify the Federal Network Agency without delay after the service has been started, accompanied by documents, of how the requirements pursuant to paragraph (2) and the statutory ordinance pursuant to sentence 1 and § 170 (5) as well as the technical directive pursuant to sentence 2 and § 170 (6) are implemented in their installations. Any changes must be notified to the Federal Network Agency without delay. The Federal Network Agency regularly reviews implementation of the requirements.

§ 3

Obligation to store and right to use traffic data to identify subscribers

(1) Any person providing internet access services shall, by assigning a public Internet Protocol address to a subscriber, store the following data:

1. the public Internet Protocol address allocated to the subscriber for an internet connection;

2. the port numbers associated with the Internet protocol address and other traffic data, insofar as these are necessary for the identification of the connection owner by means of an Internet protocol address assigned at a certain time,

3. a unique identifier for the connection used to access the internet, as well as an assigned user ID and

4. the date and exact time (to the second) of the start and end of the allocation of public Internet Protocol addresses, together with the associated port numbers and other traffic data – insofar as such data is required to be stored in accordance with point 2 – on a subscriber, specifying the relevant time zone in each case.

The data referred to in the first sentence shall be stored for three months each. Content of communications, as well as data on access to or use of other telecommunications or digital services, shall not be stored on the basis of this provision.

(2) A provider pursuant to paragraph (1) sentence 1 who does not generate or process all of the data to be stored pursuant to paragraph (1) sentence 1 itself shall:

1. ensure that the data not produced or processed by it itself during the provision of its service are stored in accordance with paragraph 1;

2. inform the Federal Network Agency immediately, upon request, of who stores this data.

(3) Obliged entities referred to in paragraph 1 shall ensure that the data retained pursuant to paragraph 1:

1. are protected against unauthorised access and use by means of state-of-the-art technical and organisational measures,

2. are stored in a manner that is technically and effectively separated from all other end-user data held by the data controller,

3. are stored in such a way that information on the subscriber can be provided to the authorised entities without undue delay; and

4. after expiry of the storage period referred to in the second sentence of paragraph 1, are erased without undue delay and irreversibly in accordance with the state of the art.

(4) The data stored pursuant to paragraph 1 may not be used:

1. for information pursuant to § 174(1), third sentence, or

2. to obtain subscriber data in accordance with Regulation (EU) 2023/1543

d) for the fulfilment of a European Production Order or

e) for a European Preservation Order preparatory to the issue referred to in (a):

using an efficient technical process which does not impair the separate storage referred to in point 2 of paragraph 3. The data stored in accordance with paragraph 1 may not be used for other purposes. For information pursuant to § 174(1), third sentence, the efficient technical procedure set out in § 174(7) must be used.

(5) The statutory instrument issued pursuant to § 170(5) may lay down provisions setting out the details of the obligations under paragraph 3, including requirements regarding the systems, procedures and technical facilities used for the storage of data under paragraph 1. Technical details for the implementation of these obligations shall be laid down in the technical guidelines pursuant to § 170(6). Obligated parties referred to in paragraph 1 must notify the Federal Network Agency without delay upon commencement of the service, providing documentation showing how the requirements set out in paragraph 3, the statutory instrument referred to in the first sentence and § 170(5), and the technical guideline referred to in the second sentence and § 170(6) have been implemented in their facilities. Any changes must be notified to the Federal Network Agency without delay. The Federal Network Agency regularly reviews implementation of the requirements.'

3. § 228 is amended as follows:

a) Paragraph 2 is amended to read as follows:

a%6) in point 38, the words 'or the second sentence of § 181' are deleted.

b%6) Point 39 is replaced by the following Point 39:

'39. contrary to § 168(1), first sentence; § 170(1)(3)(a), § 170(2)(2) or § 170(3), first sentence; § 176(4), third or fourth sentence; or § 177(2)(2) or § 177(5), third or fourth sentence, fails to make a notification, or makes a notification that is incorrect, incomplete or not made in good time,'.

c%6) Points 56 to 60 are replaced by the following Points 56 to 60a:

‘56 contrary to § 174(6) sentence 1 does not transfer data or transfers data incorrectly, incompletely, fails to transfer data on time,

1. fails to maintain confidentiality contrary to § 174(6), second sentence, read in conjunction with § 175(4), or contrary to § 176(3),

2. fails to ensure that data are protected, contrary to § 176(2)(1) or § 177(2)(1) or (3)(1),

3. fails to ensure, contrary to § 176(2)(2) or (3) or § 177(3)(2) or (3), that data is stored in the manner specified therein,

4. fails to ensure that data is deleted, contrary to § 176(2)(4) or § 177(3)(4),

60a. does not store data, or does not store them for the prescribed period, contrary to the first or second sentence of Paragraph 177(1),’.

b) Paragraph 6 is amended as follows:

a%6) In point 2, the entry '54 and 57 to 59' is replaced by the entry '54, 56, 58, 60 and 60a'.

b%6) In point 3, the entry '50, 53 and 60' is replaced by the entry '50, 53 and 59'.

c%6) In point 5, the entry ‘56’ is replaced by the entry ‘57’.

4. After § 230(16), the following Para. 17 is inserted:

‘(17) The provisions of § 177 shall be complied with by... [insert: six months after the date of entry into force referred to in Article 13 of this Law] at the latest.’

Artikel 7

Amendment of the Telecommunications Interception Ordinance

The Telecommunications Interception Ordinance in the version published on 11 July 2017 (Federal Law Gazette I p. 2316), last amended by Article 11 of the Act of 9 January 2026 (Federal Law Gazette 2026 I No. 7), is amended as follows:

1. § 2 is amended as follows:

a) Point 1(b) is replaced by the following Point (b):

‘(b) within the meaning of Part 4, the order to provide information on traffic data pursuant to § 100g(1) to (4) in conjunction with § 101a(1), first sentence, point 1, of the Code of Criminal Procedure, § 20(1), first sentence, point 5, of the Military Shield Service Act, § 8a(1), first sentence, point 4, of the Federal Act on the Protection of the Constitution, also in conjunction with § 3(1) of the Act on the Federal Intelligence Service, § 52(1) of the Federal Criminal Police Act, § 25(1) of the Federal Police Act, § 77(1) of the Customs Investigation Service Act or pursuant to Land law;’

b) Point 3(b) is replaced by the following Point (b):

‘(b) within the meaning of Part 4, the body entitled under § 100g in conjunction with § 101a(1) and (5) and § 100a(4), first sentence, of the Code of Criminal Procedure, § 20(1), first sentence, point 5, of the Military Shield Service Act, § 8a(1), first sentence, point 4, of the Federal Act on the Protection of the Constitution, also in conjunction with § 3 of the Act on the Federal Intelligence Service, § 52 of the Federal Criminal Police Office Act, § 25(1) of the Federal Criminal Police Act, § 77 of the Customs Investigation Service Act or under Land law pursuant to the relevant order, to make requests for information on traffic data pursuant to § 3(70) of the Telecommunications Act;’

2. In the first sentence of § 32(1), the words ‘and the Telecommunications Digital Services Data Protection Act’ shall be inserted after the words ‘Telecommunications Act’.

3. § 35 is amended as follows:

a) In the second sentence, the words ‘or the Telecommunications Digital Services Data Protection Act’ are inserted after the words ‘Telecommunications Act’.

b) Point 4 of sentence 3 is replaced by the following point 4:

'4. an indication of the legal basis on which the traffic data accessed was retained;'.

Artikel 8

Amendments to the Telecommunications Digital Services Data Protection Act

The Telecommunications Digital Services Data Protection Act (TDDDG) of 23 June 2021 (Federal Law Gazette I p. 1982; 2022 I p. 1045), as last amended by Article 3 of the Law of 10 March 2026 (Federal Law Gazette 2026 I No.64) is amended as follows:

§ 13a is replaced by the following § 13a:

‘§ 13a

Compliance with obligations pursuant to Articles 10 and 11 of Regulation (EU) 2023/1543

(1) Providers of telecommunications services and the addressees established by them pursuant to § 3(1) to (3) of the Electronic Evidence Implementation and Enforcement Act are allowed to process personal data to the extent necessary to comply with a European production order or a European preservation order pursuant to Regulation (EU) 2023/1543, as amended on 12 July 2023. Secrecy of communications (Article 10(1) of the Basic Law) is restricted in this respect.

(2) '§ 176(2)(2) to (4) of the Telecommunications Act shall apply mutatis mutandis to personal data secured in accordance with paragraph 1, with the proviso that the data must be deleted immediately and irreversibly as soon as data retention is no longer required under Regulation (EU) 2023/1543.'

Artikel 9

Amendment to the Federal Police Act

The Federal Police Act … [Article 1 of the Draft Act Modernising the Federal Police Act, Bundestag document 21/3051] is amended as follows:

1. In the table of contents, the following is inserted after the reference to § 25:

   '§ 25a: Retention of traffic data'.

2. § 25 is amended as follows:

   a) In paragraph 1, the words ‘pursuant to § 3(70) of the Telecommunications Act’ shall be inserted after the words ‘traffic data’ in the information before point 1.

   b) Paragraph 4(2) is replaced by the following Paragraph 4(2):

      ‘2. the telephone number or other identifier of the line or terminal concerned, unless it is clear from certain facts that it is also associated with another terminal, or, when securing data from a radio cell, if otherwise achieving the purpose of the measure would be hopeless or significantly more difficult, a sufficient description of the telecommunication in terms of space and time;’

   c) Paragraph 5, sentence 2, point 2 is replaced by the following point 2:

      ‘2. the telephone number or other identifier of the line or terminal concerned, unless it is clear from certain facts that it is also associated with another terminal, or, when securing data from a radio cell, if otherwise achieving the purpose of the measure would be hopeless or significantly more difficult, a sufficient description of the telecommunication in terms of space and time;’

   d) Paragraph 6 is replaced by the following Paragraph 6:

      ‘(6) The party obliged to provide information pursuant to paragraph 1 or 2 shall provide the data required for the provision of information without delay and in full. Whether and to what extent arrangements are to be made for this purpose shall be determined in accordance with the Telecommunications Act and the Telecommunications Interception Ordinance.’

3. After § 25, the following § 25a is inserted:

‘§ 25a

Preservation of traffic data

(1) For the purpose of any collection of traffic data pursuant to § 25(1), the Federal Police may order that obliged entities pursuant to § 25(1) must immediately secure traffic data of data subjects if the data subject is personally or spatially related to the danger or crime to be prevented pursuant to § 25(1) and

1. there are factual indications that the person in question is a person within the meaning of § 25(1) and that collection pursuant to § 25(1) could be justified, or

2. there is actual evidence to suggest that the person in question is associated with a person referred to in § 25(1)(2) or (3) in a manner that goes beyond mere fleeting or incidental contact, and in a way that justifies the assumption that, once further information has been obtained, an investigation under § 25(1) might be warranted.

The data must be relevant for the purposes specified in § 25 (1).

(2) The order referred to in the first sentence of paragraph 1 may only be issued by the President of the Federal Police Headquarters or a Federal Police Directorate, their deputy, or the head of a department of the Federal Police Headquarters. The order is issued without hearing the person concerned. The order shall take effect upon issue. It shall be issued in writing. It must include the following:

1. the person against whom the measure is directed, including, where possible, their name and address,

2. the telephone number or other identifier of the line or terminal concerned, unless it is clear from certain facts that it is also associated with another terminal, or when securing data from a radio cell, if otherwise achieving the purpose of the measure would be hopeless or significantly more difficult, sufficient description of the telecommunication in terms of space and time;

3. The nature, scope and duration of the action, specifying the end point;

4. the nature of the data to be collected by the measure and their likely importance for the purpose of the collection; and

5. the main reasons.

The order shall be limited to a maximum period of three months. The court may grant an extension of no more than three months at a time, upon application by the person authorised to issue the order under the first sentence, provided that the conditions for the order continue to be met in light of the information obtained. The local court with jurisdiction is the one in whose district the authority of the person entitled to make the application under the first sentence has its registered office. The provisions of Book 1 of the Act on Proceedings in Family Matters and in Matters of Non-contentious Jurisdiction shall apply mutatis mutandis to these proceedings, with the exception of § 23(2), § 37(2) and § 41. If the conditions for the order are no longer met, the measures taken pursuant to the order must be terminated immediately.

(3) The party obliged on the basis of an order pursuant to paragraph 1 shall immediately and fully preserve the data covered by the order. The second sentence of § 25(6) and paragraph 7 shall apply accordingly.'

Artikel 10

Amendment to the Law on associations

The Vereinsgesetz (Law on associations) of 5 August 1964 (Federal Law Gazette I p. 593), as last amended by Article 5 of the Act of 30 November 2020 (Federal Law Gazette I, p. 2600), is amended as follows:

§ 4(4) is amended as follows:

1. Sentence 1 is replaced by the following sentence:

   'The provisions of § 94 to 97, § 98(4) and § 99, § 100 and § 101 of the Code of Criminal Procedure shall apply mutatis mutandis to the seizure of items that may be relevant as evidence.'

2. Sentence 4 is replaced by the following sentence:

   '§ 104, § 105(2) and (3), § 106 to § 110, § 111c, § 111n to § 111p of the Code of Criminal Procedure shall apply accordingly.'

Artikel 11

Amendment to the Money Laundering Act

The Money Laundering Act of 23 June 2017 (Federal Law Gazette I p. 1822), as last amended by Article 53 of the Act of 04 February 2026 (Federal Law Gazette 2026 I No. 33) is amended as follows:

In § 29(2a), second sentence, point 2, the words '100k(1), second sentence, §§' are replaced by the words '100k,'.

Artikel 12

Restriction of a fundamental right

Article 1(2) and (3), Article 6(2) and Article 9(3) restrict telecommunications secrecy (Article 10(1) of the Basic Law).

Artikel 13

Entry into force

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

EU legal acts:

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings and the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118)

Justification

A. General part

I. Objective and necessity of the regulations

Social life is now inconceivable without the digital realm. This development also affects crime. Criminal offences often have a digital dimension, for example when two suspects communicate with each other via a messaging service to plan a terrorist attack. Or the crimes take place completely in a digital environment, for example by perpetrators disseminating child pornography or operating a trading platform on which narcotics and cybercrime-as-a-service (CaaS) are offered, or by selling goods that do not exist at all in a real-life online shop (fake shops).

Law enforcement and other investigative authorities already have the tools to follow the digital trail left by criminals on the internet. In particular, they can collect data from telecommunications services – such as Internet access services – and digital services – such as social network operators.

However, data is often fleeting. In the case of crimes committed on or via the internet, perpetrators usually leave behind the Internet Protocol (IP) address they used as a trace. Assigning this address to a subscriber – especially in the case of crimes committed exclusively on the Internet – is often the only investigative approach. If a law enforcement agency or other authorised body wishes to identify the subscriber associated with an IP address, it submits a subscriber information request to the internet service provider. However, the search will be successful only if the provider is still storing the link between the IP address and the subscriber. This is the case only for a few days, if at all, as internet access service providers so far only store this data to the extent and for as long as it is necessary for their operational purposes. As a result, many investigations come to nothing, or the authorities are forced to resort to other investigative methods that are far more resource-intensive and, in some cases, more intrusive.

In the past, there have been several attempts to introduce data retention of traffic and location data for law enforcement and security purposes, most recently with the Act on the introduction of a storage obligation and a maximum retention period for traffic data of 10 December 2015 (Federal Law Gazette I, p. 2218). In a preliminary ruling procedure initiated by the Federal Administrative Court, the Court of Justice of the European Union ruled, in its judgement of 20 September 2022 – C-793/19 and C-794/19, Spacenet and Others – that regulations such as those introduced in Germany in 2015 are incompatible with EU law. As a result, the Federal Administrative Court ruled on 14 August 2023 – 6 C 6.22 – that the relevant provisions of the Telecommunications Act are incompatible with European law and may no longer be applied. By order of 22 June 2017 – 13 B 238/17 – the Higher Administrative Court for the Land of North Rhine-Westphalia (Oberverwaltungsgericht für das Land Nordrhein-Westfalen) () had already provisionally held, in favour of an internet access service, that there was no obligation to store its customers' traffic data on the basis of the law introduced in 2015.

In order to enable law enforcement authorities and other authorised entities to reliably identify subscribers by means of an IP address, it is necessary, but also sufficient, to introduce an obligation to store IP addresses. This preventive storage of IP addresses falls within the scope of what the European Court of Justice deemed permissible in its judgement of 30 April 2024 (Case C-470/21, Quadrature du Net II – Hadopi). Inventory data query, already possible today, will thus become many times more productive. This

provides the authorities with a tool that enables them to follow what is often the only, but almost always the first, most efficient and quickest investigative approach.

Furthermore, the instrument of a preservation order is created for traffic data. This allows law enforcement authorities and the Federal Police to order the preservation of traffic data if and as long as the legal or factual conditions for data collection for law enforcement purposes are not yet met. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (Evidence Regulation) presupposes the existence of the Preservation Order tool for law enforcement purposes in national law. Its introduction is therefore also relevant in cross-border cases.

Furthermore, there is a need to clarify what threshold applies to cell site query. In its ruling of 10 January 2024 – 2 StR 171/23 – the Federal Court of Justice ruled that a mobile phone cell site query requires there to be a suspicion of a particularly serious criminal offence. The threshold is now laid down by law to the effect that a criminal offence of significant importance is sufficient.

II. Main content of the draft

The draft adapts the powers of the law enforcement authorities to the requirements of the present in a moderate manner.

Under the draft, internet service providers will, firstly, be required to retain for three months the IP addresses they assign to end users, along with other data such as the port number, insofar as this is necessary to uniquely identify the IP address with a subscriber. This allows law enforcement authorities and other authorised entities to query the inventory data from the internet access service provider on the basis of a time stamp, an IP address and, if applicable, a port number, provided that the legal requirements for this are met. The draft thus meets an essential need of the authorities. The data retention requirement applies to all users of internet access services in Germany. However, data does not allow anything other than subscriber identification by means of an IP address. It is precisely not data retention of all traffic and location data. In particular, it is not possible to create browsing or activity profiles from stored IP address data. The adverse effect on innocent users in particular is therefore manageable. At the same time, this takes the pressure off the authorities, as the retrieval of inventory data is an investigative tool that is capable of providing a valuable lead with relatively little effort. Otherwise, they would have to take much more time-consuming measures, such as conducting research on the open internet (OSINT searches). Not only do these measures often fail to yield results, but they can also affect law-abiding citizens and, in some cases, involve a greater intrusion into privacy than simply checking existing records. Under this draft, retrieval of inventory data during preliminary investigations will be more promising and can be carried out in a targeted manner.

The introduction of a storage obligation is in line with constitutional law. The preventive storage solely of telecommunications traffic data necessary to identify the subscriber associated with a dynamic IP address that has been identified by other means constitutes a significantly less intrusive measure than the near-complete storage of data relating to all telecommunications connections (see Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 257). The draft is designed in such a way that it takes into account the weight of the intervention associated with the storage obligation.

The introduction of the storage obligation is compatible with European Union law. In its current form, it does not constitute a serious interference and is justified by the objective of combating criminal offences (see European Court of Justice, judgement of 30 April

2024, Case C-470/21, Quadrature du Net II – Hadopi, paragraphs 82 et seq., 101 and 115).

Secondly, the draft provides for the introduction of the instrument of the preservation order. This enables law enforcement agencies and the Federal Police to order telecommunications companies to preserve traffic data even if the legal requirements for collection have not (yet) been met for legal or factual reasons. Since the instrument can be used quickly, there is the prospect that the authorities will be able to prevent the deletion of volatile data in connection with a specific, known crime and thus access this data in the future for their further investigations.

Thirdly, it expressly provides that cellular searches are permitted for offences of major importance, in particular under § 100a(2) of the Code of Criminal Procedure (StPO). This was the prevailing practice in criminal proceedings until a ruling by the Federal Court of Justice on 10 January 2024 – 2 StR 171/23. The draft measure re-enables this practice.

The draft also abolishes the provisions on data retention contrary to European law and the associated powers to access such data. The draft also provides for a systematic reorganisation of § 100g, § 100j and § 100k of the Code of Criminal Procedure, as well as the related procedural provisions contained in § 101a of the Code of Criminal Procedure.

The amendment to the Judicial Remuneration and Compensation Act (JVEG) ensures that companies required to implement a preservation order are adequately compensated for the costs they incur in each individual case.

The subsequent amendments to the Telecommunications Act (TKG) and the Telecommunications Interception Ordinance (TKÜV) serve to regulate the storage, transmission and deletion obligations for providers of telecommunications services resulting from the new preservation order.

In addition, the law contains mainly consequential adjustments in other laws.

III. Executive footprint

In the development phase, the internet access service providers with their own networks (Deutsche Telekom AG, Telefónica Germany GmbH & Co. OHG, Vodafone GmbH and 1&1 Telecommunication SE) were consulted on the technical feasibility of the proposed regulations. The content of the draft has not been significantly influenced by statements made by the company's representatives.

IV. Alternatives

None.

V. Legislative powers

The legislative competence of the Federation derives from Article 74(1)(1) of the Basic Law (judicial proceedings), point 3 (association law) and from Article 73(1)(5) (border protection), (6) (air transport), (6a) (railways) and (7) (telecommunications).

VI. Compatibility with European Union law and international treaties

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

Under the conditions set out in the draft, the preventive retention of IP addresses falls within the scope of what the European Court of Justice deemed permissible in its judgement of 30 April 2024 (Case C-470/21, Quadrature du Net II – Hadopi).

The introduction of a preservation order also adapts national criminal procedure law to Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Article 6 of the Regulation provides for a European Preservation Order. Under Article 6(3), a decision may be issued only if it could have been issued in a comparable national case under the same circumstances. The provisions under German law take into account the requirements set out by the Court of Justice of the European Union for a preservation order, as set out in particular in its judgement of 6 October 2020 (Joined Cases C-511/18, C-512/18 and C-520/18, Quadrature du Net I). In particular, the preservation order is issued on a case-by-case basis and is limited in scope.

Furthermore, Article 16 of the Council of Europe Convention on Cybercrime, known as the Budapest Convention, which has been signed and ratified by Germany, contains a provision requiring signatory states to empower the competent authorities to order the immediate preservation of traffic data. This obligation will be implemented with the introduction of the preservation order.

VII. Impact of the legislation

1. Legal and administrative simplification

The Telecommunications Act repeals the provisions on data retention that are incompatible with European law. This also applies to the power to summon witnesses referred to in the Code of Criminal Procedure. This leads to simplification of the law. In addition, the powers of the law enforcement authorities regulated in the Code of Criminal Procedure for the retrieval of inventory, traffic and usage data are recast as a whole and are thus more manageable in practical terms.

2. Sustainability aspects

The intended introduction of the preservation order contributes to the achievement of Goal 16 'Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels' of the 2030 Agenda for Sustainable Development. This Sustainable Development Goal, through its targets 16.1, 16.2, 16.4 and 16.5, calls for significant reduction in all forms of violence and violence-related mortality everywhere, an end to all forms of violence against children, the combating of all forms of organised crime, and a substantial reduction in corruption and bribery. Precautionary IP address storage and the preservation order contribute to achieving these objectives by enabling the collection and exploitation of digital traces that were not previously accessible to law enforcement to this extent.

The draft thus follows the principles of the German Sustainability Strategy ‘(1) Apply sustainable development as a guiding principle at all times and in all decisions’, ‘(2) Assume global responsibility’ and ‘(5) Preserve and enhance social cohesion in an open society’.

3. Budget expenditure excluding compliance costs

The following additional expenditure is expected in the federal budget. Requirements are calculated in accordance with the guidelines for estimating expenditure and (plan-) posts in the federal budget.

In the budget of the Federal Ministry of the Interior, section 06, the Federal Office for the Protection of the Constitution will incur additional personnel and material costs from the financial year 2027. The necessary technical adjustments to the IT infrastructure (network connections, network technology, electronic interfaces) will incur one-off capital expenditure of around €254,000 in the 2027 financial year. Annual material costs of EUR 177 000 will be incurred for day-to-day operations from 2027 onwards. According to current estimates, the necessary technical adjustments and day-to-day operations will require an additional four (planned) posts (1 A14, 1 A12, 1 A11, 1 E9a). The additional annual personnel costs amount to EUR 372 000.

Under the budget of the Federal Ministry of Justice and Consumer Protection, section 07, minimal additional operational costs will be incurred by the Federal Court of Justice (BGH) and the Federal Public Prosecutor at the Federal Court of Justice (GBA) from 2027 onwards. It can be assumed that the Federal Court of Justice (BGH) and the Federal Public Prosecutor's Office (GBA) issue a total of around three preservation orders per year. Given that the average cost of compensation under items 500 to 507 and 600 of Annex 3 to the JVEG amounts to 105 euro, the projected additional material costs amount to well under 1 000 euro per year.

No additional material costs or personnel costs are to be expected in the budget of the Federal Ministry of Finance. The additional staffing requirements for the customs administration (Customs Investigation Service and Customs Criminal Investigation Office) amount to less than 0.5 posts in total and therefore cannot be determined with any greater precision.

Additional expenditure set out above, as well as any other additional expenditure, is to be offset in terms of both funding and staffing within the relevant budget section.

In the budget of the Federal Ministry for Economic Affairs and Energy, section 09, the Federal Network Agency has an estimated additional staff requirement of 26.0 posts (1 A16, 1 A15, 1 A14, 1 A13gZ, 3 A13g, 5 A12, 5 A11, 1 A10, 1 A9mZ, 2 A9m, 3 A8, 1 A7, 1 A6m) for supervisory tasks and for additional administrative fine proceedings from financial year 2027 onwards. For specialised tasks, additional annual personnel costs totalling EUR 2.376 million, direct material costs of EUR 891 000 and overheads of EUR 960 000 are therefore incurred. The additional horizontal tasks require a further 7.8 posts (respectively 0.3 A16, A15, A14 and A13gZ, 0.9 A13g, 1.5 A12 and A11, 0.3 A10 and A9mZ, 0.6 A9m, 0.9 A8 and 0.3 A7 and A6m). Additional personnel and material costs for cross-cutting tasks are included in overheads.

To this must be added one-off material costs of EUR 25 000 in 2027 for the extension of the existing laboratory facility and annual material costs of EUR 5 000 from the 2027 financial year onwards.

In section 09, additional revenue is also to be expected from additional administrative fine procedures. The amount of revenue depends on the number of fine proceedings and the amount of fines imposed. They therefore cannot be predicted.

Additional requirements in terms of posts are to be offset in Section 09. The additional financial requirements are to be offset in the relevant sections in terms of funding and staffing.

Overall, the regional budgets are expected to show a shortfall of €1.429 million. The projected additional costs for providing further information on existing data, amounting to approximately 172,000 euro (11 773 additional requests × 15 euro in compensation under paragraph 201 of Annex 3 to the JVEG), and the additional costs for preservation orders, amounting to 120 000 euro (1,134 orders x average compensation of €105 pursuant to point 500 to 507 and 600 of Annex 3 to the JVEG) are offset by savings resulting from the

reduced compensation rate for inventory data queries (57 367 annually) from €45 to €15 in accordance with point 201 of Annex 3 to the JVEG. These savings are expected to amount to around EUR 1.721 million.

This is not expected to have any impact on local authority budgets.

4. Compliance costs

a) Compliance costs for citizens and businesses

None.

b) Compliance costs for the authorities

None.

5. Other costs

The regulations on IP address storage and the introduction of a preservation order for traffic data concern the judicial core area. It can be assumed that the implications will be largely cost-neutral for both the federal government and the Länder. There are additional costs for the economy. However, effects from this on individual prices and the general price level, in particular the consumer price level for telecommunications services, are not anticipated. In detail:

a) Federal state government

aa) Radio cell query

No significant additional workload is expected in relation to the radio cell query. Until January 2024, the prevailing view was that the measure could be applied in cases of serious offences, in particular those under § 100a(2) of the Code of Criminal Procedure. The draft now makes this explicitly clear.

bb) IP address storage

With regard to the disclosure of inventory data under § 100j(2) of the Code of Criminal Procedure, it is to be expected that the number of requests for such information will increase as a result of the introduction of a three-month retention period for IP addresses. However, given the immediate costs involved, it can be assumed that the draft will be cost-neutral.

Only the compensation obligations referred to in point 201 of Annex 3 to the JVEG shall be regarded as direct material costs. The expected increase in the number of requests for information does, however, give rise to additional compensation obligations. However, this is offset by the reduction in the compensation amount from 45 euro to 15 euro per piece of information.

There is no broad data base available to estimate the future increase in the volume of requests for information. The federal states were unable to say in how many procedures an inventory data disclosure using an IP address would have been carried out in the past if a three-month storage obligation had already existed. For the most part, they were also unable to provide any information on how many requests for inventory data had been made in how many proceedings, or whether such requests would have been legally permissible in principle. There are no plans to collect these figures statistically; conducting a retrospective survey would have involved a disproportionate amount of effort.

However, an estimate can be made based on the figures estimated by North Rhine-Westphalia for inventory data information requests for the years 2023, 2024 and 2025. Based on the figures stored in the Infreq100 IT system, the state of North Rhine-Westphalia has estimated that in 2024 there were 13,277 (2023: 13 144; 2025: 11431) inventory data information queries for law enforcement purposes. The data queries in question, based on the criterion of an IP address (BDA-IP), are carried out by local police via the Electronic Interface for Public Authorities (ESB) – in this case, the IT procedure Infreq100 – provided that the parties subject to the obligation are also required to participate in the ESB under the Telecommunications Interception Ordinance (TKÜV) or are connected to it. Based on experience in North Rhine-Westphalia, the number of BDA-IP queries not made via the ESB is negligible. The Infreq100 overview of BDA-IP data does not provide a breakdown by individual criminal investigations, so it is not possible to say in how many different criminal investigations these queries were made. For the purposes of a nationwide estimate of the number of inventory data requests, it should therefore be assumed that one request was made per procedure. This is also consistent with the empirical data provided by telecommunications providers, which indicate that typically one identifier is requested per procedure. If one compares the 13 277 queries from 2024 with the total number of cases received by the public prosecutor's offices in North Rhine-Westphalia this year (1 270 996), this results in a percentage of 0.0104461383. Extrapolating from the nationwide figures for 2024 (5,491,712), the estimated number of requests for subscriber data based on IP addresses made by the state law enforcement authorities in 2024 is 57,367.

The federal states unanimously expressed the view that the introduction of a three-month IP address retention period is likely to result in a significant increase in the number of requests for information. Some indication of the extent of the increase can be found in the Federal Criminal Police Office's 2022 investigation into actual and hypothetical success rates in investigations there, according to information from the National Centre for Missing & Exploited Children (NCMEC) (see the Federal Criminal Police Office's position paper of 21 July 2023 on the required retention periods of IP addresses, available at https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html or also the Federal Criminal Police Office's opinion of 5 July 2023 on Bundestag document 20/3687, available at https://www.bundestag.de/resource/blob/970516/Stellungnahme-Link_BKA.pdf).
According to this, in around 24 per cent of the 66 000 cases examined, the IP addresses transmitted were older than eight days (around 15 600 processes) at the time the information sheet was received. Assuming that, in these cases, no request for subscriber data was made from the outset, the proportion of cases in which a request for subscriber data based on an IP address would have been made had a three-month retention obligation been in force would be 24 per cent. However, it should also be taken into account that the NCMEC processes are not representative of all procedures in which access to inventory data on the basis of an IP address is possible as a investigative approach. In other proceedings, the IP addresses may be considerably older by the time the law enforcement authorities become aware of possible criminal conduct (see also the explanatory notes to Article 6(2) regarding § 177(1) of the Telecommunications Act).

If, on this basis, we apply a generous estimate of an increase of around 20 per cent when estimating the additional volume of requests for inventory data, this would result in an additional 11,473 requests for information in 2024, based on the figures mentioned above. Multiplied by EUR 15 in accordance with the amended point 201 of Annex 3 to the JVEG, this results in an amount of EUR 172 095. If we take as our basis the empirical figure provided by telecommunications providers – namely that one identifier is typically queried per transaction – this results in an additional cost of €172 095, which will have to be funded from the budgets of the federal states. However, this is offset by the reduction in the previous compensation amount under paragraph 201 of Annex 3 to the JVEG from 45 euro to 15 euro, which, based on an estimated nationwide figure of 57 367 requests for access to inventory data via IP address by the law enforcement authorities of the federal

states for 2024, results in savings of 1 721 million euro. Given the requests for information that are already possible under the current legal framework – based on the estimated number of requests for inventory data for 2024 – a significant reduction in the administrative burden is expected in future. It is true that the amount of EUR 45 referred to in point 201 of Annex 3 to the JVEG is currently foreseen for up to ten identifiers requested simultaneously in the same procedure, which form the basis for the provision of information, whereas the draft provides for an amount of EUR 15 for only up to three identifiers requested simultaneously in the same procedure. However, given the experience reported by telecommunications providers that typically only one identifier is queried per procedure, this fact has no practical impact.

There will be no immediate additional staffing costs that could not be covered by existing staff. In particular, a key prerequisite for the disclosure of inventory data is the existence of an initial suspicion, which must be assessed at the stage of initiating proceedings.

A further effect of the draft is that requests for information based on an IP address will be more often successful in the future and thus lead to further investigative approaches that entail corresponding costs as indirect effects (further investigations and possible judicial proceedings). It is not possible to put a figure on these costs, as it is impossible to predict in how many cases the additional requests for information, combined with which further investigative measures, will lead to charges. In addition, each procedure can develop a different scope depending on the circumstances of the individual case. However, if one compares the figure of 11,473 additional requests for information with the 561,539 new criminal proceedings filed with courts nationwide in 2024, then – assuming that each additional request for information would lead to a successful investigation – an increase of no more than 0.02 per cent could be expected, which falls within the usual annual fluctuations.

It is not possible to quantify with certainty the other costs incurred by the Land police authorities in their security function and by the intelligence services of the Länder. However, it should be noted that, based on the figures reported by North Rhine-Westphalia, queries for personal data for the purpose of preventing danger account for only a small proportion of those made for the purposes of criminal prosecution (in North Rhine-Westphalia in 2024, there were a total of 13,485 queries for personal data, of which 208 were for the purpose of preventing danger). Against this background, and given the reduction in the flat-rate fee for this type of information, any additional costs are likely to be minimal, if any.

cc) Preservation order

It is reasonable to assume that, in cases involving domestic matters, the investigative tool of the preservation order will be used to a lesser extent than the measures for collecting data under § 100g(1) to (4) of the Code of Criminal Procedure, because in many such cases the conditions for collecting the data relevant to the individual case under § 100g(1) to (4) of the Code of Criminal Procedure are likely to be met. In 2024, a total of 22 684 measures under § 100g of the Code of Criminal Procedure were implemented by the law enforcement authorities of the Länder. Of these, a total of 15 955 were radio cell queries. Assuming that the volume of preservation orders amounts to an estimated 5 per cent of 22 684, then, in view of the direct material costs arising from the compensation obligations under paragraphs 500 to 507 and 600 of Annex 3 to the JVEG, an additional burden on the state budgets totalling approximately 120 000 euro would be expected.

Another consequence of the draft is that the preservation order may also lead to further investigative measures, which, as indirect effects, may entail additional costs, namely further investigations and any subsequent legal proceedings. As in the case of precautionary IP address storage, these costs cannot be quantified either. However, if one compares the estimated figure of around 567 preservation orders with the 561,539 new

criminal cases brought before the courts nationwide in 2024, then – assuming that each preservation order results in a successful investigation – an increase of no more than 0.001 per cent could be expected, which falls within the usual annual fluctuations.

In addition to safeguarding data, the instrument can also generate savings – the exact amount of which cannot be quantified – by making other, more resource-intensive measures (such as OSINT activities) unnecessary, measures which might otherwise have been carried out.

The legal instrument of the European Preservation Order, on the other hand, could be of higher practical relevance. This assumption is based on the fact that data may be secured by the public prosecutor's office – in emergencies pursuant to Article 4(5) of Regulation (EU) 2023/1543 – whereas, in the case of European Production Orders concerning traffic data, judicial authorisation is required and the public prosecutor's office cannot be granted emergency powers under the provisions of Regulation (EU) 2023/1543 (see Bundestag document 21/3192, page 44). The time-saving advantage this offers can be decisive in cross-border cases and may lead to German authorities increasingly making use of the legal instrument of the preservation order when they wish to secure data in other Member States. However, it is not possible to estimate the percentage of cases in which this can reasonably be assumed. This is an entirely new legal instrument, which is why there is no existing experience with it. Nor is it possible to derive figures from outgoing requests for the collection of traffic data, as no statistics exist in the area of other forms of mutual legal assistance, and outgoing requests that are not also executed domestically are not included in the national statistics under § 101b of the Code of Criminal Procedure.

It is not possible to put a reliable figure on the additional costs incurred by the regional police authorities.

b) Federal Government

aa) Judicial authorities, customs administration, police authorities and intelligence services

(1) Radio cell query

No significant additional workload is expected in relation to the radio cell query.

(2) Precautionary IP address storage and preservation order

To the Federal Public Prosecutor and the Federal Court of Justice (investigating judge)

The comments on the federal states apply accordingly. In 2024, the Federal Public Prosecutor at the Federal Court of Justice initiated a total of 65 proceedings under § 100g of the Code of Criminal Procedure. In view of the preservation order, only a minor additional burden is to be expected on this basis.

To the customs administration

Disclosure of inventory data in proceedings conducted by the Customs Investigation Service: The investigations of the customs investigation service are regularly directed against serious and organised crime. According to the Customs Investigation Service, the possibility of retroactively querying IP addresses from internet access service providers for three months is expected to increase the number of requests. It is estimated that each customs investigation office will handle 100 additional enquiries per year, which, with eight customs investigation offices, amounts to 800 cases. The result is ultimately a slight increase in staff costs, the exact amount of which cannot be quantified.

Preservation orders in cases handled by the Customs Criminal Investigation Office: Depending on the significance of the case, or if a customs investigation office requests it, or if the Federal Public Prosecutor issues a corresponding investigation order, the Customs Criminal Investigation Office conducts the criminal investigation itself. Depending on the facts of the case, it may be necessary to evaluate the traffic data of accused persons and other persons. In such cases, an order to preserve traffic data should be issued at an early stage, if necessary, so that it can be obtained during subsequent proceedings. This results in minor additional personnel costs, which cannot be quantified.

Preservation orders in procedures conducted by customs investigation offices: Investigations by customs investigation offices are regularly directed against serious and organised crime. Gang-related offences are the norm. Investigators from the Public Prosecutor's Office working within the Customs Investigation Service require the power to issue preservation orders at an early stage of the investigation in order to secure communications data relating to potential suspects and other individuals involved in an offence. The result is ultimately a slight increase in staff costs, the exact amount of which cannot be quantified.

The Customs Administration does not incur any expenditure affecting the budget in the performance of its security functions.

On the police authorities

In the context of the Federal Criminal Police Office's remit (to counter the threat of international terrorism) under § 5 of the Federal Criminal Police Office Act (BKAG), it can be assumed that, despite the expected increase in the number of queries, the authority to retrieve subscriber data using IP addresses pursuant to § 40(4), first sentence, of the BKAG will not result in higher operational costs for the Federal Criminal Police Office. Ultimately, the number of inventory data collections depends on the number of security operations initiated per year, which cannot be reliably estimated and is subject to fluctuations. Based on current estimates, the expected increase in the volume of stock data queries can be handled by the existing staff. Furthermore, this Act reduces the flat-rate fee for this type of information (see paragraph 201 of Annex 3 to the JVEG), meaning that no additional costs are expected for the time being.

The same applies to the Federal Criminal Police Office's remit under § 6 of the Federal Criminal Police Office Act (protection of members of constitutional bodies and the leadership of the Federal Criminal Police Office) and the power to retrieve subscriber data using IP addresses pursuant to § 63a(4)(2) of the Federal Criminal Police Office Act (number of instances of subscriber data retrieval using an IP address in 2022: 162).

In the context of the Federal Criminal Police Office's remit under § 2 of the Federal Criminal Police Office Act (BKAG), it can currently be assumed that the authority to query master data using IP addresses to determine local jurisdiction in the federal states pursuant to § 10(3) of the BKAG will not result in any increased operational costs for the Federal Criminal Police Office, despite an expected rise in the volume of queries. According to current estimates, no additional staff will be required (number of inventory data collections based on an IP address in 2022: 86 250). Furthermore, as the connection can now be identified on the basis of the IP address, this will reduce the additional workload previously incurred at the central office in determining local jurisdiction for a case through more complex or time-consuming measures. Even taking into account the flat-rate fee for this type of information that is to be set in future, no additional administrative costs are expected at this stage.

In the context of the Federal Police's remit, and given the flat-rate fee to be established in future for the power to query subscriber data using IP addresses in accordance with § 22a(3), first sentence, of the Federal Police Act, it can be assumed that, despite the

expected increase in the volume of queries, no higher operational costs will be incurred by the Federal Police. According to the current assessment, there will also be no need for additional staff. With regard to the preservation order under § 25a(1) of the Federal Police Act, only a minor additional burden is to be expected.

In accordance with Section 100j of the Code of Criminal Procedure (StPO) and Section 4 of the Federal Criminal Police Office Act (BKAG), the Federal Criminal Police Office will increase its requests for subscriber data to identify offenders based on IP addresses. Despite the expected increase in the volume of enquiries, it is currently assumed that this will not result in higher operational costs for the Federal Criminal Police Office. According to the current assessment, no additional staff will be required. The same applies to preservation orders in criminal proceedings.

On the intelligence services

Due to the expected increase in the number of queries regarding existing data, resulting from the longer retention period for IP addresses, the Federal Office for the Protection of the Constitution will need to automate the process, which has hitherto been carried out manually. For the technical implementation, one senior and two general officials are required. This takes into account necessary adjustments in the field of grid transitions, network technology and system extensions to the TKÜ systems for the automation of the new queries from the TKÜ inventory systems as well as technical adjustments to the ESB. At the same time, it must be ensured that there is no leakage of classified data. Similarly, the corresponding responses must be linked back to the respective queries in the telecommunications surveillance system. An additional function is required in mD to handle the technical work involved in implementing the new query options. The Federal Office for the Protection of the Constitution will therefore require an additional four (planning) posts (1 senior, 2 general, 1 junior officials). The resulting personnel costs amount to around EUR 395 000 per year. The Federal Office for the Protection of the Constitution will also incur material costs of around €254 000 (one-off) and around €177,000 (annual).

It is not possible to put a reliable figure on the additional costs incurred by the Federal Intelligence Service.

bb) Federal Network Agency

The Federal Network Agency is expected to incur further costs.

The group of persons subject to these obligations is defined in § 176 and 177 of the Telecommunications Act. These are, pursuant to § 176 of the Telecommunications Act, providers of publicly available telecommunications services and, pursuant to § 177 of the Telecommunications Act, providers of internet access services. On the basis of these obligations, the Federal Network Agency estimates, based on the notifications under § 5(1) of the Telecommunications Act (TKG), that there are around 3,000 entities subject to the obligations under § 176 TKG and around 700 entities subject to the obligations under § 177 TKG.

Pursuant to § 176(4) and 177(4) of the Telecommunications Act (TKG), the Technical Guidelines issued under § 170(6) of the TKG set out the technical details of the various obligations and stipulate that the parties subject to these obligations must notify the Federal Network Agency immediately upon commencing operations of how the requirements are being implemented; any changes must be notified without delay. In addition, under these regulations, the Federal Network Agency reviews the implementation of the requirements after initial implementation, in the event of changes and regularly at intervals of about two years.

As a result of these regulations, the Federal Network Agency will then be responsible for the following tasks:

The development, establishment and updating of requirements for the separate and secure storage of traffic data subject to retention or storage obligations, as well as for the secure transmission of orders and traffic data, in accordance with the Technical Guidelines under § 170(6) of the Telecommunications Act. In this context, both relevant national guidelines, such as those issued by the Federal Office for Information Security, and international standards must be taken into account. In order to keep pace with the latest developments, the specifications must be continuously reviewed and updated. The guidelines are drawn up in consultation with the relevant authorities and with the involvement of trade associations and manufacturers. To carry out this task, one graduate and three graduates with a background in information technology are required.

Receipt and review of the documentation relating to the implementation of the requirements, as well as verification of the actual technical and organisational implementation across all approximately 3,000 obligated parties. In addition, regular checks on the implementation of the legal obligations are carried out at intervals of about two years. At 220 working days per year, this results in a review of seven obliged entities per day. In order to carry out these audit activities and the associated administrative procedures, a high level of human resources is required. To complete this task, 1 senior, 10 general and 8 junior officials are required.

Enforcement of the above-mentioned obligations under § 228 TKG and § 230(16) TKG. This will require additional work to handle the necessary administrative offence procedures. Enforcement proceedings pursuant to § 183(1) of the German Telecommunications Act (TKG) may also be considered to enforce undertakings' obligations. To perform this task, 1 senior and 2 general officials are necessary.

In total, the Federal Network Agency requires a staffing level of 26 staff units to carry out its tasks, comprising 3 senior officials, 15 general officials and 8 junior officials. The resulting personnel costs amount to around EUR 1.727 million per year. The Federal Network Agency also incurs material costs of around EUR 25 000 (one-off) and around EUR 5 000 (annually).

c) Businesses

The telecommunications companies concerned incur additional costs as a result of complying with the data retention obligations associated with a preservation order and those provided for in § 177(1) of the Telecommunications Act, as well as the further requirements under § 176(2) and § 177(2) of the Telecommunications Act.

Unlike previous regulations on comprehensive data retention, only an indiscriminate storage obligation with regard to IP addresses is introduced, as well as an event-related obligation to secure traffic data on the basis of a preservation order in specific criminal proceedings.

As the storage obligation applies without distinction to all providers of internet access services, approximately 700 undertakings are affected. When considering the estimated costs, a distinction must be made between the initial investment required to set up the technical measures for data collection and secure storage, and the ongoing costs of continuously updating these systems. The situation can vary widely for individual companies. If companies already store IP addresses for a certain period of time for operational reasons, it might be sufficient for them simply to extend these periods by technical means. For companies that do not currently store IP addresses for operational purposes, the costs of initial set-up and ongoing maintenance are correspondingly higher.

For companies that assign public IP addresses to several subscribers simultaneously using Network Address Translation (NAT) methods and therefore also have to store port numbers and, if necessary, other data in order to identify a subscriber, it should be noted that these data are usually not available outside the NAT systems used. In these cases, these NAT systems must first be replaced, which represents a significant intervention in the companies' active networks and correspondingly entails additional costs.

In addition, all providers of telecommunications services must make technical and organisational arrangements for the security and provision of traffic data. This applies in particular to the establishment of storage infrastructure enabling identification data to be stored for up to three months or longer and subsequently deleted, including integration into existing processes. Approximately 3 000 companies are affected by the arrangements.

The procedure for securing and handing over data differs from the requests for information currently made for the purposes of criminal prosecution – which companies are required to respond to under existing law – in terms of the requirements regarding data protection and erasure. In this respect, there is a significant additional burden involved in securing and disclosing traffic data, which affects all telecommunications service providers without exception.

Some associations and companies state that, depending on whether NAT procedures are used or not, and depending on the details of the protection and deletion measures to be determined, the implementation of the storage obligation could entail one-off investment costs of EUR 1 to 2 million for large providers, EUR 150 000 to 200 000 for medium-sized providers and EUR 80 000 for small providers. According to this information, running costs amount to an average of 10 per cent of investment costs. According to estimates by some large companies, personnel costs could be between EUR 200 000 and EUR 550 000; no concrete information is available for medium-sized or smaller companies.

For the implementation of the security and disclosure of traffic data, some companies state that, depending on the protective measures to be determined, one-off investment costs of EUR 60 000 to EUR 300 000 are necessary for large providers and EUR 30 000 for small providers. Running costs were indicated at up to 40% of the initial investment. Personnel costs could also be between EUR 100 000 and EUR 250 000 for large suppliers and around EUR 10 000 for smaller suppliers.

Associations and companies that have commented on the costs emphasise that, given the need for each organisation to adapt its internet access network to collect the data, and given that the requirements for security measures have yet to be finalised, these are merely current, rough estimates.

The major providers estimate that it takes around 30 to 60 minutes per case to process the retrieval and subsequent disclosure of traffic data; for the disclosure of subscriber details based on an IP address, they estimate it takes around 10–15 minutes. It should be noted that this expenditure may be reimbursed in accordance with Annex 3 to the JVEG. The compensatory measures provided for in Article 4 of this draft cover this expenditure.

6. Other legal consequences

The planned regulations have no impact on consumers. The provisions are neutral with regard to gender equality policy. No demographic effects are expected.

VIII. Time limit; evaluation

No time limit for the provisions is envisaged. They concern core areas of criminal procedure law and associated telecommunications law, and are designed to be long-term in nature, not least because of the technical implementation they require.

No separate documentation is required. Precautionary IP address storage serves only to identify a subscriber on the basis of an IP address and thus constitutes an interference with fundamental rights that cannot be regarded as serious (see European Court of Justice, judgement of 30 April 2024, Case C-470/21, Quadrature du Net II – Hadopi, paragraph 90), so an evaluation is not necessary in this respect. It is unnecessary for the introduction of the preservation order, as it also serves to implement Regulation (EU) 2023/1543. In addition, statistical recording is planned anyway, so that the benefits can be continuously tracked.

B. Specific part

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

In the Code of Criminal Procedure, the provisions on inventory data retrieval (§ 100j), traffic data retrieval (§ 100g) and usage data retrieval (§ 100k) as well as the procedural provisions related thereto (§ 101a) are revised. These regulations concern the powers of law enforcement authorities to collect various types of data from providers of telecommunications services and providers of digital services. The revision is necessary because the regulations have become increasingly complex as a result of a series of legislative reforms in recent years. This applies in particular with regard to § 100k, introduced in 2021, which concerns the collection of usage data: The provision contains rules similar to those in § 100g, but is structured and worded differently in some respects. In this respect, systematic adjustments are being made. In addition, the current § 100g(2), which regulates the grounds for retrieval of retained data, is deleted due to the incompatibility of the provisions on data retention with European law. In addition, § 100g(4) introduces new provisions governing the retrieval of cell site data, and § 100g(7) introduces, for the first time, an order for the preservation of traffic data.

Re Point 1 (Table of contents)

These are consequential editorial amendments to point 3 (recast of § 100j) and point 4 (recast of § 101a).

Re Point 2 (§ 100g – Collection of traffic data)

The provision is recast.

The current paragraph 2 contains a list of offences for the collection of retained traffic data. It is to be repealed. This follows the judgement of the Federal Administrative Court of 14 August 2023 (6 C 6.22), which, following a preliminary ruling by the Court of Justice of the European Union (judgement of 20 September 2022 – C-793/19 and C-794/19, Spacenet and Others), ruled as follows: The obligation laid down in § 175(1), first sentence, in conjunction with § 176 of the Telecommunications Act (TKG) – § 113a(1), first sentence, in conjunction with § 113b TKG (old version) – regarding the obligation of providers of publicly available telecommunications services to store the telecommunications traffic data specified therein is wholly incompatible with Article 15(1) of Directive 2002/58/EC and is therefore inapplicable, because it prescribes the indiscriminate, comprehensive and undifferentiated retention of a large proportion of traffic and location data in terms of personnel, time and geography is prescribed and – insofar as EU law does not preclude limited data retention from the outset – the requirements

regarding the specificity and clarity of the provision, the permissible purposes and the further substantive and procedural requirements are not met. The current paragraph 2 relates to the collection of data from this data retention provision, which is contrary to European law, and must therefore be repealed to rectify the situation. Insofar as paragraph 2, in its current version, still refers to the third sentence of paragraph 1 with regard to the collection of stored location data, different conditions will apply in future; see the explanatory memorandum to paragraph 3 for further details.

Paragraph 1 now contains the basic offence of traffic data collection. The issue of data retrieval in connection with criminal offences committed via telecommunications is now governed by paragraph 2. The rules on location data retrieval (paragraph 3) and radio cell retrieval (paragraph 4) build on the requirements of paragraph 1 as specific forms of traffic data retrieval. Paragraph 5 introduces a new power to collect certain traffic data from number-independent interpersonal communications services with a view to subsequently identifying the accused person. Paragraph 7 introduces the power to issue a preservation order.

The existing paragraph 4 will not be retained. The provision expressly prohibits the collection of traffic data from the retention of data relating to persons bound by professional secrecy. This provision is no longer necessary, as it relates to the collection of data from data retention provisions that contravene European law and are being abolished. As these rules have never been enforced, their removal does not alter the level of protection afforded to those bound by professional secrecy. The protection of persons bound by professional secrecy, including the protection of journalist sources, is – as hitherto – guaranteed under the general protection provision of § 160a. The newly introduced obligation to retain IP addresses and associated data is in no way connected to the collection of traffic data under § 100g; rather, it merely implements the existing provision for retrieving subscriber data under § 100j(2). It is not possible to obtain any information from the inventory data regarding those with whom those bound by professional secrecy have communicated. This is because the only information that may be requested is the identity of the subscriber associated with an IP address that has come to the attention of the law enforcement authorities.

Consequently, the level of protection afforded to media professionals remains unchanged. As far as the European Media Freedom Act (EMFA) contains guarantees for the protection of media professionals, these must – as before – be taken into account as a matter of priority when applying the law.

Regarding § 100g (Collection of traffic data)

Re Paragraph 1

Re Sentence 1

The provision sets out the basic case for the collection of traffic data from those who provide or contribute to publicly available telecommunications services, § 100g(1), first sentence, point 1, and second sentence of the current version. The provision has been redrafted without any significant changes to the legal situation.

With regard to the concept of traffic data, current legislation refers to § 9 and § 12 of the Telecommunications and Digital Services Data Protection Act (TDDDG). For systematic reasons, this reference is replaced by a reference to the statutory definition in § 3(70) of the Telecommunications Act. This does not, therefore, entail any change in the legal position. It is expressly clarified that data from the precautionary storage of IP addresses pursuant to § 177 of the Telecommunications Act cannot be collected directly as traffic data on the basis of § 100g(1). Law enforcement authorities may only request information regarding the subscriber associated with an IP address in accordance with § 100j(2).

The provision makes it clear for the first time that the addressee of the measure is the accused. This is already in line with the current legal position; see § 101a(1), first sentence, in conjunction with § 100a(3). The term ‘accused’ continues to include – as before – suspects whose names are not yet known, i.e. where proceedings are initially brought against persons unknown (see, regarding § 100a, Federal Court of Justice, order of 8 February 1994 – 1 BGs 88/94).

Newly included in the provision is for the first time expressly who can be obliged with an order. To date, the relevant data subjects have been identified only indirectly through the wording of the references to collectable traffic data in the Telecommunications and Digital Services Data Protection Act and in the Act on the Establishment of a Federal Agency for Digital Radio for Authorities and Organisations with Security Responsibilities. Now, in the first sentence, those who offer or participate in publicly available telecommunications services are expressly designated as obliged entities. The wording is based on § 100j(1), first sentence, point 1, which permits the retrieval of inventory data and explicitly identifies the parties subject to this obligation. § 100g(1), first sentence, continues to prohibit the submission of requests to telecommunications providers that do not offer publicly available telecommunications services (see Bundestag document 19/4671, p. 61; Rückert, in: Munich Commentary on the Code of Criminal Procedure, 2nd edition 2023, § 100g, paragraph 42). These include, for example, operators of wireless networks (WLANs) in hotels.

The explicit designation of suitable obliged entities in § 100g does not entail any change in the legal situation. Law enforcement authorities are therefore not limited to collecting data only with the cooperation of the obligated party. For example, in the case of an IP tracking measure carried out by an investigating authority itself, the collection of traffic data can still be based on § 100g (cf. Federal Court of Justice, decision of 23 September 2014 – 1 BGs 210/14).

The new first sentence of § 100g(1) also contains, in catalogue format, the substantive requirements for the consultation of traffic data. Point 1 contains, as before, the requirements for the system. Point 2 provides that, where necessary, the collection of traffic data is permitted not only for the purposes of investigating the facts of the case, as has been the case hitherto, but also for the purpose of determining the whereabouts of the accused. With regard to the requirement of proportionality in point 3, the current legal situation also continues to apply.

Re Sentence 2

The second sentence includes the possibility that, in addition to the traffic data of the accused, data may also be collected from persons for whom it is reasonable to assume, on the basis of certain facts, that they will receive or pass on certain messages intended for or originating from the accused or that the accused will use their connection or IT system (news intermediaries). This provision also currently applies (§ 101a(1), first sentence, in conjunction with § 100a(3)). This is not a procedural provision, but rather a provision defining the scope of application; consequently, incorporating it into the enabling provision is appropriate for systematic reasons.

Re Sentence 3

The third sentence of the new version expressly states that the Federal Agency for the Digital Radio of the authorities and organisations with security responsibilities may also be obliged entities. This adaptation does not lead to any change in the legal situation either (see also Bundestag document 19/4671, page 61).

Re Paragraph 2

The provision now specifically regulates the power to collect communications data in cases where there is a suspicion of a criminal offence committed via telecommunications that is not already covered by § 100g(1), first sentence. Crimes committed by means of telecommunications do not have to be crimes of considerable importance also in individual cases; this is in line with the current legal situation. This separate provision simplifies the basic elements set out in paragraph 1 and the specific measures relating thereto concerning location data and cell site queries.

The collection of traffic data will be permitted in future if investigation of the facts would otherwise be hopeless or significantly more difficult. This represents a slight relaxation of the subsidiarity clause, as, until now, recourse to it has only been permitted where research would otherwise be futile (§ 100g(1), second sentence, current version). The amendment is intended to harmonise the powers of collection (see § 100a(1), first sentence, point 3, § 100b(1), point 3, § 100c(1), point 4, § 100f(1) and (2) and § 100h(2), second sentence, point 2).

There is no need for an explicit provision stating that a measure under paragraph 2 does not authorise the collection of location data. This follows from the new system of provisions, under which the collection of location data (paragraph 3) is only permitted under the conditions set out in paragraph 1 – and therefore specifically not under those of paragraph 2.

Re Paragraph 3

The rules on location data retrieval are moved to a separate paragraph and rearranged. For the first time, express reference is made to the legal definition in § 3(56) of the Telecommunications Act. There is therefore no change in the legal situation.

In future, the same conditions will apply to the retrieval of existing location data and data that will be collected in the future or in real time. The conceptual distinction can therefore be dispensed with.

Under § 100g(1), third sentence, of the current version of the law, access to existing location data is only permitted under the strict conditions set out in the applicable paragraph 2; that is, where there is a suspicion of a particularly serious criminal offence, provided that establishing the facts of the case or determining the whereabouts of the suspect would otherwise be significantly more difficult or futile. However, the retrieval of location data that will be generated in the future, or in real time, is currently permitted under the less stringent requirements of the applicable paragraph 1, sentence 1, point 1, namely where there is a suspicion of a criminal offence of significant importance in the individual case, provided that the measure is necessary for the investigation of the facts or for determining the whereabouts of the suspect. This distinction stems from the fact that, originally, location data was to be retained for four weeks without any specific reason. Collection was considered particularly sensitive, as it could also have been used to create movement profiles for bystanders. By contrast, the collection of future location data and real-time location data was classified as less sensitive, as it did not rely on stored data (see Bundestag document 18/5088, page 27).

In fact, the retention of location data has never been enforced and has since been declared inapplicable by the Federal Administrative Court on the grounds that it infringes EU law (see the general section of the grounds under I. for further details). In fact, retrieving existing (historical) location data therefore often yields very little information, as those required to provide such information store the data solely for operational purposes. Data are usually deleted after seven days at the latest. It is not possible to generate activity profiles covering a period of several weeks using these data. It is therefore justified

to permit the retrieval of location data under paragraph 3 in its entirety, subject to the conditions set out in the new paragraph 1, that is, where there is a suspicion of a criminal offence of significant importance in the individual case.

Conversely, a moderate increase in the intervention conditions is required for the retrieval of future location data. This is because this investigative tool would enable law enforcement agencies to compile a constantly updated movement profile – albeit only from the moment the measure is ordered or takes effect. From now on, the retrieval of future location data – just like the retrieval of existing location data – is subject to the principle of subsidiarity; it may therefore only be used where investigating the facts of the case or determining the accused's whereabouts would otherwise be significantly more difficult or impossible.

Re Paragraph 4

The provision includes the power to access mobile phone base station data, which is currently set out in § 100g(3).

According to the current legal situation, radio cell retrieval is only permitted, inter alia, under the conditions laid down in the applicable paragraph 1, sentence 1, point 1. For a long time, judicial practice has interpreted the provision to mean that such a request is permissible provided there is a suspicion of a criminal offence that is of significant importance, even in the specific case (for example, Stade Regional Court, order of 26 October 2018 – 70 Qs 133/18 – and Arnsberg Regional Court, order of 29 April 2019 – 2 Qs-410 UJs 254/19-43/19). In its ruling of 10 January 2024 – 2 StR 171/23 – the Federal Court of Justice ruled that a mobile phone cell site query requires there to be a suspicion of a particularly serious criminal offence in accordance with § 100g(2). Various regional courts have not followed the view of the Federal Court of Justice (inter alia, Landgericht Hamburg (Regional Court, Hamburg), order of 6 June 2024 – 621 Qs 32/24; Landgericht Düsseldorf (Regional Court, Düsseldorf), order of 19 June 2024 – 1 Qs 1/24; Landgericht Regensburg (Regional Court, Regensburg), order of 5 September 2024 – 8 Qs 30/24); they also consider that it is sufficient to suspect an offence of considerable importance, including in individual cases.

The new provision in paragraph 4 refers to the conditions set out in paragraph 1, thereby allowing for suspicion of a criminal offence to suffice even where the offence is of significant importance in the individual case. This is in line with current practice up to the Federal Court of Justice ruling. There is therefore no difference between the initial offence and the consultation of existing location data. This is also appropriate in the case at hand: Both instruments concern position data. They are also roughly comparable in their degree of intrusiveness. Cell site queries have a wide scope and may, in particular, also capture bystanders using their mobile phones in a given cell site at a specific point in time. However, the query does not allow for any major inference, except that a subscriber was connected to the mobile network at a certain point in time in a certain radio cell. The location data search, on the other hand, may, if data are available when the search is carried out, allow conclusions to be drawn about movements. However, the greater intrusiveness involved is offset by a much narrower scope, as the measure applies directly to a single subscriber.

The legal situation remains unchanged in that only data that has already been produced can be collected. The collection of future traffic data in a radio cell is therefore still not possible on the basis of paragraph 3. This differs – again in line with the current legal situation – from the collection of location data under paragraph 3, under which both existing and future data can be collected and real-time collection is also permitted.

The existing requirement of subsidiarity (paragraph 4 in conjunction with paragraph 3) is retained, meaning that the measure remains permissible only insofar as establishing the

facts of the case or determining the whereabouts of the accused would otherwise be futile or significantly more difficult. This takes into account the sometimes significant scope of the measure, which also includes bystanders.

Re Paragraph 5

A new provision is introduced in paragraph 5 granting the power to collect certain traffic data from number-independent interpersonal communication services (OTT-1 services; see paragraph 7, first sentence, below for further details) with the aim of subsequently identifying the suspect. The provision is modelled on the current § 100k(3) (§ 100k(4) of the new version), which already allows such collection in relation to digital services. It concerns a case common in practice where the criminal prosecution authority already knows about content relevant to procedures, for example because it has been made aware of it by means of a criminal complaint accompanied by a screenshot. Under the current § 100k(3), the public prosecutor’s office may, in such cases, collect usage data from digital services solely for the purpose of identifying the user, without the need for a court order. In practical terms, this involves finding out the IP address assigned to the user. On the basis of this data, the law enforcement authority may carry out a subscriber data query with an internet access service provider in accordance with § 100j(2) and, where necessary, identify the owner of the connection from which the service was used.

For the conditions set out in the first sentence to be met, the law enforcement authority must already be aware of the nature of the use of the service. This is in line with the already applicable requirement in § 100k(3). A new feature compared with the current § 100k(3) is that this power is not vested solely in the public prosecutor’s office, but in all law enforcement authorities, including investigators working on behalf of the public prosecutor’s office. This is appropriate, as the identification data to be collected is not particularly sensitive and merely enables the retrieval of subscriber data from the internet service provider, which investigators are already permitted to do.

Unlike in the current § 100k(3), the data that may be collected is now explicitly specified, namely stored IP address, exact time of use and, where necessary, any further data required for identification based on the IP address, such as the port number. This is based on § 177(1), first sentence, of the Telecommunications Act (TKG) as amended; reference is made to the explanatory memorandum in this regard. However, the provision does not permit the collection of personal data such as usernames, account names, email addresses or telephone numbers; in such cases, collection would be governed by § 100j.

The provision does not impose any obligation on providers to retain data; the request therefore always relates solely to data held by the provider.

Sentence 2 stipulates that the second sentence of paragraph 1 applies mutatis mutandis, meaning that the measure may also be applied in relation to news agencies. Reference is made to the explanatory memorandum for paragraph 1 sentence 2.

Re Paragraph 6

The provision is identical to the current paragraph 5, which has been moved to paragraph 6.

Re Paragraph 7

Re Sentence 1

Paragraph 7, first sentence, introduces new provisions regarding the preservation order for traffic data.

Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the enforcement of custodial sentences following criminal proceedings (the E-Evidence Regulation) also provides for a preservation order mechanism for cross-border cases within the EU. A European preservation order can be issued for all criminal offences if it could have been issued in a comparable national case under the same conditions, Article 6(3) of the e-Evidence Regulation. It is only once the European preservation order has been issued for purely domestic cases that national law enforcement authorities are able to use the European preservation order for measures taken in other European countries. Specific provisions concerning the application of the E-Evidence Regulation are set out in the Electronic Evidence Implementation and Enforcement Act (Article 3).

The need for the introduction of a preservation order arises from the fact that traffic data in particular are volatile. Telecommunications companies often store data for operational purposes for a maximum of seven days. For this reason, there is a need for an instrument which, even if the conditions for collecting traffic data are not yet met, can prevent the loss of such data.

Preservation may be ordered in the event of subsequent collection. In this sense, the preservation order is an accessory security instrument:

The preservation order may therefore be issued to all those who would also be obliged to produce the data, i.e. all telecommunications providers. These include, on the one hand, providers of number-based interpersonal telecommunications services, in particular internet access services, as well as services consisting wholly or predominantly in the transmission of signals, such as transmission services used for machine-to-machine communication and broadcasting (see § 3(61) TKG). On the other hand, providers of number-independent interpersonal telecommunications services (over-the-top-1 services or OTT-1 services, such as providers of email and messenger services) are also obligated parties (see § 3(40) TKG). OTT-1 services often replace conventional telecommunications services. For example, the SMS is replaced by messages via messenger services or the telephone call is replaced by a voice call via an app. The inclusion of OTT-1 services in the circle of obliged entities is therefore appropriate.

The group of obligated OTT-1 services also includes email providers. A preservation order against them may include, for example, the following details:

– Data relating to logins to the email account (IP address with port and timestamp, accurate to the second and including time zone) as well as location data, where applicable,

– routing information, i.e. the data from the email header,

– Display name and identifier, i.e. the email address, of the other communication participants as well as timestamp for the receipt and sending of the respective email.

An ancillary preservation order may only relate to traffic data, but – like the main measure, the collection referred to in paragraphs 1 to 4, itself – not to content data. In the case of indications of an offence committed by means of telecommunications which do not fulfil the conditions laid down in paragraph 1, an ancillary preservation order may be issued only in respect of traffic data, but not in respect of location data, since collection itself may also relate only to traffic data and not to location data (see paragraph 2 and the explanatory notes thereto).

An preservation order will regularly refer to pre-existing data. However, where the data collection measure also permits the collection of future data or real-time data – such as

the collection of location data under paragraph 2 – this shall apply mutatis mutandis to the preservation order.

The ancillary nature of the preservation order is also reflected in the restricted use of the secured data. The data collected may be used exclusively for the relevant surveillance operation; for further details, see the explanatory memorandum to the amendment to the Telecommunications Act, Article 2(2), regarding § 176(1).

The persons to whom the preservation order is addressed are the persons concerned. In this respect, the preservation order differs from the investigative measures referred to in paragraphs 1 to 4, which may only be directed against the accused or a communications provider. This takes account of the fact that, at the early stages of an investigation, the roles of the individuals involved (the suspect, an informant or a person not directly involved in the offence) are often not yet clear.

Re Point 1

In accordance with point 1, the issuing of a preservation order requires there to be sufficient factual evidence that a criminal offence referred to in paragraphs 1 to 4 has been committed. There must therefore be an initial suspicion based on specific facts, going beyond vague indications and assumptions (Köhler and Schmitt, in: Schmitt/Köhler, Code of Criminal Procedure, 68th edition 2025, § 98a, margin note 7; § 152, margin note 4). This level of suspicion corresponds to that required for a dragnet investigation (§ 98a).

This lowers the threshold set out in paragraph 1(1), which requires that certain facts must give rise to a suspicion that a person has committed an offence listed therein, either as the perpetrator or as an accomplice. Qualified suspicion directed against a certain person often arises only in the course of further investigations.

The immediate seizure of communications data may therefore be ordered at the point at which initial suspicions are still unspecified, i.e. typically immediately after the discovery of a criminal offence. Further details do not yet have to be established for the admissibility of the preservation order. This is in line with the case law of the Court of Justice of the European Union (judgement of 5 April 2022, Case C-140/20 – Commissioner of An Garda Síochána, paragraph 91).

A preservation order may only be issued where there are grounds to suspect a criminal offence of significant gravity (paragraph 1(1), where applicable in conjunction with paragraph 3 or paragraph 4) or a criminal offence committed by means of telecommunications (paragraph 2(1)). There is also a need for a preservation order for the latter configuration. This is because, in the case of offences committed by means of telecommunications, the collection of traffic data is often the only investigative approach. There would be a 'risk of systemic impunity' (see European Court of Justice, judgement of 30 April 2024, Case C-470/21, Quadrature du Net II – Hadopi, paragraph 119) if there were no adequate investigative tools in this regard.

Re Point 2

A personal or geographical link to the offence, in particular to the victim or the scene of the crime, is necessary but also sufficient for a person to be regarded as a data subject (see also the judgement of the Court of Justice of the European Union of 6 October 2020, Cases C-511/18, C-512/18 and C-520/18 – La Quadrature du Net and Others, paragraph 165). Thus, the preservation order can have a certain range. However, since the collection of data in accordance with the second sentence is only permissible if the evidence has accumulated to the point of giving rise to a reasonable suspicion against a specific suspect, the intrusion involved is of a manageable nature.

Re Point 3

A preservation order may be issued in accordance with point 3 to the extent that the data may be relevant for the purposes referred to in paragraphs 1 to 4. Unlike in the case of data collection, it is therefore not necessary for the retention of data to be required for the purposes specified in the relevant provision (paragraph 1(2)), nor is it necessary for the investigation of the facts to be otherwise futile or significantly impeded (paragraph 2(2) and paragraph 3).

The criterion of 'being of potential relevance' is based on the existing provisions concerning the securing and seizure of items for evidential purposes in § 94(1) and the examination of electronic storage media in § 110(3) (potential evidential relevance). In future, the established interpretation found there will also be applied in the context of point 2. Accordingly, it is sufficient that, at the time the preservation order is issued, there is a possibility that the communications data may be used for the purposes set out in paragraphs 1 to 4 (investigating the facts of the case or determining the whereabouts of a suspect). In this respect, it is considered sufficient to expect, in the sense of an ex ante forecast, that the traffic data will allow conclusions to be drawn regarding relevant facts; however, it need not yet be established for which specific lines of argument they may be relevant, or whether they will in fact become relevant at a later stage. However, a preservation order will be ruled out if, at the time the order is made, it is already clear that the evidence is of no significance (see, in this regard: Köhler, Schmitt/Köhler, Code of Criminal Procedure, 68th edition 2025, § 94, margin note 6 et seq.; Hauschild, in the Munich Commentary on the Code of Criminal Procedure, 2nd edition 2023, § 94, margin notes 21 and 22, each with further references). This is the case, for example, if the existence of a procedural impediment has already been established with certainty. However, the exclusion may also apply to cases where it is clearly foreseeable that the conditions for subsequent collection of traffic data in accordance with paragraphs 1 to 4 will not be met.

Re Sentence 2

Sentence 2 makes it clear that paragraph 7 does not itself confer any power to collect data. The law enforcement authority must therefore submit a separate request for information to the data controller in order to retrieve all or part of the stored data. Data may only be collected to the extent that the necessary conditions are met; in particular, this means only to the extent that the collection of data is necessary.

It is to be expected that the preservation order will generally precede the (possible) recovery. It is also conceivable, however, that the preservation order is issued at the same time as proceedings are initiated. This is relevant in cases where the legal requirements for data collection have already been met, but the data cannot yet be retrieved for technical reasons. This is of practical significance in situations where the obligated party is not required to make any arrangements for cooperation. This is because such an obligation applies only in certain cases (see § 101a(5) of the new version in conjunction with § 100a(4), second sentence). This does not include, in particular, providers of number-independent interpersonal telecommunications services (OTT-1 services). For these data subjects, the method of data collection is determined on a case-by-case basis, which may take some time. This is the case, for example, when the collection of traffic data is arranged on a server or with an email provider. In such cases, the court may order the debtor to provide security until the levy can actually be carried out.

Re point 3 (§ 100j – Collection of inventory data and § 100k – Collection of usage data)

The amendments relate to the provisions on the retrieval of inventory data in § 100j and the provisions on the retrieval of usage data in § 100k.

Regarding § 100j (Collection of inventory data)

The amendments are essentially editorial in nature. The heading is reworded and aligned with § 100g (collection of traffic data) and § 100k (collection of usage data).

Re Paragraph 1

As before, this provision, in accordance with § 100j(1), first sentence, governs the basic requirements for the disclosure of subscriber data, namely the collection of subscriber data from telecommunications service providers (point 1) and digital service providers (point 2). The text merely clarifies that the levy is to be collected 'from' these liable parties; the previous wording of the Act referred to a levy collected 'by' the party providing the relevant services.

The references to § 174(1), first sentence, of the Telecommunications Act (manual information procedure for telecommunications service providers) and to § 22(1), first sentence, of the Digital Services Act (information procedure for digital service providers) are no longer included. These references are for information only and entail no change in the legal situation.

The power to collect special data pursuant to § 100j(1), second and third sentences, has been moved to § 100j(3) without any substantive changes.

Re Paragraph 2

As before, this paragraph governs the power to request information on subscriber data on the basis of an IP address assigned at a specific point in time. Such information is currently only provided on the basis of data, in particular IP addresses, which telecommunications companies store anyway for operational purposes. At present, enquiries are generally only successful if the IP address was assigned no more than seven days ago, as data is not usually stored for longer than that. The newly introduced three-month data retention obligation under § 177 of the Telecommunications Act will mean that, in future, requests for information made to telecommunications providers within this period will generally be successful.

The request for information under § 100j(2) is compatible with constitutional law. In particular, there is no need for restrictive lists of offences containing trigger offences (Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 261; Order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 177). The authorities themselves do not have access to the data that is to be stored as a precautionary measure without any specific cause. They do not retrieve them themselves, but only receive information about the holder of a particular connection who has been identified by the service providers using this data. However, the significance of this data remains very limited: The use of data stored as a precautionary measure merely reveals which subscriber was logged on to the internet via an IP address that is already known, perhaps having been identified by other means. Although such a request involves a greater degree of intrusion, its formal structure bears a certain resemblance to a query regarding the owner of a telephone number. In any case, its intelligence value remains localised. Systematic investigations over a prolonged period or the creation of personality and movement profiles cannot be carried out solely on the basis of information derived from IP addresses at the source of a connection (see Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 256; Order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 169). However, information must not be sought on a whim: As with any investigative measure, there must be reasonable initial suspicion based on the facts of the individual case, since, in preliminary investigations, unfounded inquiries aimed at establishing suspicion are not permitted (see Kölbel/Ibold, in: Munich Commentary on

the Code of Criminal Procedure, 2nd edition 2024, § 160 paragraph 71; Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, paragraph 261; order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119-238, paragraph 145.

If the port number is also known, it should be included in the request along with the timestamp and IP address. Only if the port number is included in the request is there a reasonable prospect that the obligated party will be able to provide the information. In some cases, however, the port number will not be known to the law enforcement authorities. In such cases too, law enforcement authorities may request information, and there is a possibility that the party subject to the obligation will be able to provide it in these circumstances as well (see the explanatory memorandum to the amendment to the Telecommunications Act, Article 6(2) regarding § 177(1)).

The processing powers of service providers corresponding to the data collection standard are set out in § 174(1), third sentence, of the Telecommunications Act (TKG) for publicly available telecommunications services and in § 22(1), third sentence, of the Digital Services Act (TDDDG) for digital services.

To date, the provision also refers to § 177(1)(3) of the Telecommunications Act. This reference should be deleted, as the provision, which was contrary to EU law, has been repealed. The current § 100j(2), second sentence, is also to be deleted; this provision stipulates that fulfilment of the conditions for a request for information under the first sentence must be logged. The provision is superfluous, as the principles of the proper keeping of files in any case require that files be complete and accurate in terms of content in order to be open to review under the rule of law. The legal and factual grounds for providing information on the register must therefore also be logged (see also Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 261; Order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 248 et seq.).

Re Paragraph 3

To date, § 100j(3) lays down procedural rules for the consultation of inventory data. These are moved to § 101a for the purposes of systematic consolidation; for further justification, see that section.

In the new version, § 100j(3) contains the provisions previously set out in § 100j(1), second and third sentences. The postponement is for organisational reasons. This does not entail a change in the legal situation.

Re § 100k (Collection of usage data by digital services)

§ 100k is substantially revised in terms of drafting and its structure and regulatory content is brought closer to § 100g. This is appropriate, as § 100k grants the power to request data from digital service providers and thus applies in a configuration that runs parallel to the request for data from providers of publicly available telecommunications services (§ 100g).

§ 100k is also similar to § 100g under applicable law: § 100g governs the collection of traffic data from telecommunications companies, whilst § 100k governs the collection of usage data from digital services. The revision of the provision eliminates discrepancies between the two standards, for which there is no apparent objective reason.

Already under the current legal situation, a login case can be opened on the basis of § 100k. This keyword refers to the situation in which the law enforcement authorities have not yet been able to identify an accused person, but have reason to believe that he or she

regularly uses a particular digital service. In such cases, law enforcement authorities may, pursuant to § 100k(1) or (2), ask the digital service provider to disclose the IP address recorded during a recent login and, where applicable, the port number used. Using the timestamp, IP address and, where applicable, port number, the subscriber can be identified by means of a query for subscriber details in accordance with § 100j(2).

Re Paragraph 1

Paragraph 1 is given an editorial adjustment. The reference to § 1(4)(1) of the Digital Services Act, which provides the statutory definition of the term ‘digital service’, may be omitted. This does not entail a change in the legal situation.

In future, the provision will refer to § 100g(1), first sentence, regarding the conditions for retrieving usage data from digital services. Under current law, the conditions for access remain unchanged; this is therefore merely a drafting simplification.

The definition of digital services also remains unchanged; it is based on § 1(4)(1) of the Digital Services Act in conjunction with Article 1(1)(b) of Directive (EU) 2015/1535. This definition specifies an 'information society service' as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. Connected smart systems in vehicles – including, in particular, navigation and emergency call systems – also fall within the scope of digital services if they constitute a service provided on an on-demand basis. Accordingly, the vehicle data generated in this process, such as location data, may constitute usage data within the meaning of § 100k(1) (see Higher Regional Court of Frankfurt am Main, order of 20 July 2021 – 3 Ws 369/21 regarding the then-applicable definition of telemedia services under § 1(1), first sentence, of the Telemedia Act, which ceased to be in force on 14 May 2024). By contrast, content data generated by the use of digital services in connected vehicles cannot be collected on the basis of § 100k(1).

As is the case with § 100g(1), under current law, queries made pursuant to § 100k(1) may also result in the collection of data from communications service providers, in addition to the usage data of the accused (see the comments on § 100g(1), first sentence, regarding the definition of the accused). This is currently derived – as in the case of traffic data collection – from § 101a(1), first sentence, in conjunction with § 100a(3). In the future, this will be regulated by a reference in § 100k(1), second sentence, to § 100g(1), second sentence.

Re Paragraph 2

New rules have been introduced regarding authority to access usage data in cases where the offence was committed via a digital service. To date, the first sentence of § 100k(2) provides for a list of offences as a further condition. The parallel provision in § 100g(2) of the new version (corresponding to the previous § 100g(1), first sentence, point 2), which concerns the collection of traffic data where there is a suspicion that a criminal offence has been committed via telecommunications, does not contain a list. The rules are thus systematically aligned. This is reflected in the reference to § 100g(2), which now applies.

According to the reference, in future, the collection of usage data in cases where a criminal offence has been committed by means of a digital service will only be allowed if investigation of the facts would otherwise be futile or significantly more difficult. This constitutes – as is the case with the corresponding collection of traffic data under § 100g(2) – a minor extension of the power to access data, as access has hitherto only been permitted where investigation by other means would be futile.

Re Paragraph 3

Paragraph 3 now regulates the retrieval of location data from the provider of a digital service. At present, it is permitted in relation to existing (retroactive) location data subject to the conditions set out in § 100g(2); otherwise, it is permitted in the case of criminal offences of significant importance in individual cases, in particular those under § 100a(2) (§ 100k(1), second and third sentences); this corresponds to the applicable conditions for the collection of location data in the context of a telecommunications service. In future, this alignment will also be reflected in the structure of the legislation, as paragraph 3 refers directly to the conditions set out in the new § 100g(3). For the new requirements, see the explanatory memorandum to § 100g(3).

For reasons of consistency, the text of the current § 100k(3) is moved to paragraph 4.

Re Paragraph 4

The provision builds on the current § 100k(3), but is adapted to the newly created § 100g(5). The relevant criteria set out therein apply mutatis mutandis; this also applies to the data set (IP address, time of storage, and any further traffic data required for identification, such as the port number; see § 100g(5) for further details), which may be collected. Refer to the justification contained therein.

Re Paragraph 5

The provision corresponds to the current § 100k(4).

Re Paragraph 6

Paragraph 6 continues the current paragraph 5. The content of the provision remains unchanged and will only be subject to minor editorial amendments: The current version focuses not only on the collection of usage data, but also on ‘content of usage’. This has not been included in the new paragraph 6 because the collection of content data is not possible under § 100k, either under the old or the new legal framework. To date, digital service has been defined by reference to § 1(4)(1) of the Digital Services Act, but this reference may be omitted (see also paragraph 1).

Re point 4 (§ 101a – Procedural rules for the collection of traffic, usage and inventory data)

§ 101a sets out all the procedural provisions relating to § 100g, 100j and 100k. This is reflected in the revised title of the standard.

The standard is reworded as a whole. The procedural rules for the disclosure of inventory data, previously set out in § 100j, will be incorporated into § 101a.

Paragraph 4, as currently in force, which sets out specific rules on the use of usable personal data collected through measures taken pursuant to the current § 100g(2), including in conjunction with § 100g(1), third sentence, or § 100g(3), second sentence, will not be retained. The introduction of the provision served to implement the Federal Constitutional Court’s rule that transfer to other bodies of personal data retained in the context of the retention of traffic and location data and transferred in the context of the collection of traffic data pursuant to the aforementioned provisions may be provided for by law only in so far as it was carried out for the performance of tasks for which access to those data would also be directly permissible (Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, paragraph 236); the provision was thus intended to prevent circumvention of the strict rules on use in Paragraph 113c(1) of the old version of the TKG (see Bundestag document 18/5088, p. 35). Since the

provisions on the retention of traffic and location data referred to in § 100g(2) of the current version are inapplicable because they are incompatible with European law and will be repealed (see the amendment to the Telecommunications Act), there is no longer any need for a corresponding special restriction on use. The restrictions on the use of collected data set out in the general provisions – namely § 161(3) and § 479(2) – apply.

The previous paragraph 5, which concerns situations where personal data has been obtained through a police measure involving data retention that contravenes European law, has also become redundant.

Regarding § 101a (Procedural rules for the collection of traffic, usage and inventory data)

Re Paragraph 1

As before, the provision contains a reference to the provisions of § 100a and 100e regarding procedural rules for data collection in relation to telecommunications and digital services. The structure of this reference is now clearer.

Re Sentence 1

The current § 101a(1) refers to § 100a(3) and (4) and to § 100e in its entirety. In this context, the reference to § 100a(3), which specifies the recipients of the measure, is unnecessary, as this provision is incorporated directly into the definition of traffic data collection, § 100g(1), second sentence; usage data collection under § 100k(1), second sentence, refers to this. The reference to § 100a(4), which concerns the obligations of service providers to cooperate, can henceforth be found in § 5.

§ 100e(2) and § 100e(3), second sentence, points 6 and 7 are no longer referred to. These provisions concern specific procedural requirements for online searches (§ 100b) and the acoustic monitoring of living spaces (§ 100c), which have no equivalent in the collection of data from service providers at issue here. For the same reason, § 100e(5) sentences 3 to 5 shall no longer be referred to. These regulations contain specific procedural provisions governing online searches under § 100b and the acoustic monitoring of residential premises under § 100c, according to which the issuing court must also be kept informed of the progress of the measure and, where necessary, may order the measure to be terminated. The reference is contained in the Act on the more effective and practical organisation of criminal proceedings of 17 August 2017 (Federal Law Gazette I 2017, p. 3202). In fact, however, only consequential editorial amendments were intended (Bundestag Paper 18/12785, page 58). Nor is it objectively necessary to involve the court on an ongoing basis following an order for the collection of traffic or usage data, as the data collection measures at issue here are not comparable in terms of the extent of their intrusion to the measures provided for in § 100b and 100c.

The reference to § 100e(4) regarding specific requirements for the grounds for issuing or extending an order may be omitted, as a separate provision exists for this in § 101a(2).

Points 1 to 3 specify the measures to which the reference to the individual provisions of § 100e applies. In addition to the measures under § 100g(1) to (4), to which the current § 101a(1) relates, the provisions also include measures under § 100k(1) and (2) and § 100g(7).

In future, appeals under § 304(1) will also be admissible in respect of the measures newly included in § 101a(1) that are based on a court decision, without the need for any further legislative amendment. This also applies if a Higher Regional Court (Oberlandesgericht) () has jurisdiction at first instance. In its current version, § 304(4), second sentence, point 1, provides in general terms that, exceptionally, an appeal may be lodged against decisions

and orders of the Higher Regional Courts having jurisdiction at first instance concerning the measures referred to in § 101a(1), including those newly introduced therein. Due to the comparable nature of the above-mentioned measures, the extension of the right of appeal is appropriate. With regard to measures that are not based on a court order – for example, where the public prosecutor's office issues a preservation order under § 100g(7) – the general rules on legal remedies apply; see also the explanatory notes to paragraph 4.

Re Point 1

The regulation sets out procedural rules for the collection of traffic data. Reference is made only to § 100g(1) to (4), which regulates the collection of different types of traffic data. Procedural arrangements for preservation orders are set out separately in point 3.

The rule laid down in (a) corresponds to point 1 of the first sentence of paragraph 1 in the version currently in force. The rule in (b) corresponds to the applicable third sentence of paragraph 1. These are purely editorial adjustments.

The current second sentence of paragraph 1 will not be retained. Accordingly, in the cases referred to in § 100g(2), including in conjunction with § 100g(3), second sentence, the provision on the public prosecutor's power to take urgent action under § 100e(1), second sentence, does not apply. This exclusion is no longer necessary, as the provisions relate to the retrieval of data from data retention schemes that contravene European law, which are being removed from the Act.

Re Point 2

This provision contains specific procedural rules for the collection of usage data pursuant to § 100k(1) to (3).

Re (a)

The measure taken here has so far been included in paragraph (1a). The provision is being amended for editorial reasons; this does not entail any changes to its content.

Re (b)

It is expressly stipulated that the operative part of the decision must also clearly specify the data to be transmitted and the period for which it is to be transmitted. This is in line with the parallel regime for the collection of traffic data set out in point 1(a).

The current paragraph 1a also contains a reference to § 100a(3), which concerns the recipients of the query; this is now regulated in identical terms in § 100k(3), second sentence, in conjunction with § 100g(1), second sentence, and may be deleted from the procedural provisions. The reference to § 100a(4), which was previously also provided for, is moved to paragraph 5 for editorial reasons.

Re Point 3

The regulation contains new procedural provisions for the preservation order under § 100g(7). As with the traffic data retrieval itself, the procedural provisions set out in § 100e also apply to the preservation order, subject to the following conditions:

Re (a)

Notwithstanding § 100e(1), first to third sentences, the Public Prosecutor's Office may itself order preservation, that is, without involving the court. In the event of imminent danger, this power is also available to their investigators. This is appropriate: The

preservation order is intended to prevent the loss of volatile data because the factual or legal conditions for its disclosure have not yet been met. Any delay must therefore be avoided. At the same time, there is no need for judicial control at this stage, as the law enforcement authorities cannot (yet) obtain the data. The impact on the individual concerned is therefore relatively minor. For this reason, by way of derogation from § 100e(1), third sentence, the preservation order does not require any subsequent judicial confirmation.

Preservation may be ordered for a maximum period of three months. Often, this will be sufficient for the law enforcement authorities to establish the query requirements. An extension may be granted once for a maximum of three months, but may only be ordered by the court at the request of the public prosecutor's office.

Re (b)

Point (b) provides that the operative part must also clearly indicate the data to be preserved and the period for which they are to be preserved. This is a specific provision concerning the legal basis for the retention of traffic data, which mirrors the provision on the collection of traffic data set out in paragraph 1(a).

Re (c)

Point (c) provides that, when data relating to a radio cell is secured, a description of the telecommunications that is strictly limited in terms of time and space and is sufficiently specific is sufficient for the purposes of the operative part; this corresponds to the provision governing the collection of radio cell data under point 1(b).

Re Sentence 2

The provision concerns the procedural rules governing the retrieval of inventory data under the revised § 100j(3), which relates to particularly sensitive data such as passwords. The procedural rules currently in force under § 100j(3) to (5) will be incorporated into § 101a(1) and simplified at the same time. Like sentence 1, sentence 2 contains a reference to the provisions of § 100e. However, this reference differs from that in the first sentence, as the measures referred to there – such as the collection of traffic data – may be of longer duration. However, in the case of an inventory data query aimed at issuing passwords, an extension of the measure is not considered. This is only logical: Passwords can only be issued once. If there is evidence that passwords have been changed or added, a new production order may be considered. This unique nature is reflected in the limited references and conditions.

With regard to the power to issue orders, the following applies: With regard to the current § 100j(1), third sentence (requests for information concerning passwords or other data collected as inventory data, by means of which access to end devices or to storage devices used within those end devices or in a separate location is protected), the current provision states that the public prosecutor's office's power to issue urgent orders does not apply, § 100j(3), first sentence. Conversely, with regard to § 100j(1), second sentence (requests for information concerning data used to protect access to end devices or to storage devices used within such end devices or in a separate location), it is provided that investigating officers may also take action in cases of imminent danger (§ 100j(3), second sentence). In the interests of simplification and harmonisation, these special arrangements will be discontinued. Instead, reference is made to § 100e(1), first sentence, which provides that, in principle, only the court may issue an order at the request of the public prosecutor's office; pursuant to § 100e(1), second sentence, the public prosecutor's office may take action in cases of imminent danger.

The provision in paragraph 1 stipulates that the court's decision must be issued without delay; this replaces § 100e(1), second sentence, under which the public prosecutor's order ceases to have effect unless it is confirmed by the court within three working days. Thus, the already applicable provision of § 100j(3) sentence 3 continues, according to which the court decision must be made immediately. No reference is made to the provisions regarding the duration and extension of the order set out in § 100e(1), sentences 4 and 5, as this is a one-off query.

The reference to § 100e does not refer to point 5 of the first sentence of paragraph 3, which concerns requirements for the decision-making formula for measures relating to a telecommunications connection. As stated at the outset, this has no equivalent in the one-off consultation of passwords. For the same reason, the provision under point 2 stipulates that the duration and end date of the measure are not to be specified in the operative part of the decision.

Measures under § 100j(2) of the amended version – that is, the retrieval of subscriber data on the basis of an IP address – are still not subject to a reference to § 100e(1) and therefore do not require judicial authorisation. In view of the clear degree of intervention, it is not required under constitutional law (see Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 261; decision of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 254) or under European law (see European Court of Justice, judgement of 30 April 2024, Case C-470/21, Quadrature du Net II – Hadopi, paragraph 132 et seq.).

Re Sentence 3

This provision incorporates the previous wording of § 100j(3), fourth sentence, according to which special procedural rules do not apply if the data subject is already aware of the request for information or ought to be aware of it, or if the use of the data has already been authorised by a court order. The purely declaratory fifth sentence of § 100j(3), which stipulates that the fulfilment of the relevant conditions must be logged, was not included. In any case, the prosecution authority in charge of the file is obliged to do so in accordance with the principle of proper management of the file (see also the statement of reasons for § 100j(2)).

Re Paragraph 2

The provision lays down specific requirements for the justification of measures and thus corresponds to paragraph 2, which is currently in force. Accordingly, the justification must set out the essential considerations regarding the necessity and proportionality of the measure on a case-by-case basis. One of the new additions to the scope of application is the preservation order under § 100g(7). Furthermore, the provisions governing access to existing data have been supplemented in relation to particularly sensitive data, in particular passwords, in accordance with § 100j(3). It is reasonable to assume that criminal procedure has already complied with this requirement, given the sensitive nature of the data; in this respect, this is merely a clarification.

The reference to § 100e(4) previously contained in § 101a(1), first sentence – which also sets out requirements for the justification of measures – may be omitted.

Re Paragraph 3

This provision regulates the obligation to label, evaluate and delete the data collected. This corresponds to the previous paragraph 3. Here too, the provision regarding the retrieval of inventory data relating to particularly sensitive data has been included in accordance with § 100j(3). The reasoning set out in paragraph 2 applies mutatis mutandis. The data collected on the basis of identification data from OTT-1 services

pursuant to the newly created § 100g(5) shall not be included. This corresponds to the current legal situation with regard to the data on the basis of an identification data consultation pursuant to § 100k(3). Furthermore, the preservation order under § 100g(7) is not included, as the data subject to the preservation order has not (yet) been collected and therefore cannot be flagged.

The second sentence of paragraph 3 of the current version, which concerns the labelling of data derived from data retention that contravenes European law, may be omitted, as the provisions relating to such data retention are being removed from the Act.

Re Paragraph 4

The provision regulates the reporting obligations.

The first sentence provides that a notification must be made in the case of traffic data collection pursuant to § 100g(1) to (5) and in the case of usage data collection pursuant to § 100k(1) to (4). This is in line with the current legal position (see paragraph 6, first sentence, and paragraph 7, first sentence), with the notification requirement for data collection under § 100g(5) modelled on that under § 100k(4).

This also covers the collection of usage data based on an IP address (§ 100j(2)) and in relation to specific data such as passwords (§ 100j(3)). Until now, a separate notification rule has applied in this regard under § 100j(4), which is being repealed for the sake of simplification. The same applies to the special notification rule in § 101a(7), first sentence, applicable to the identification data query pursuant to § 100k(3), applicable version (paragraph 4, new version).

Sentence 2 refers to § 101(4), sentences 2 to 5, and paragraphs 5 to 7 for further provisions regarding the duty to notify, which concern notification in the case of covert measures. The reference corresponds to the second sentence of paragraph 6, which previously applied to the collection of traffic data and usage data with regard to special data such as passwords. The current requirements – namely that a decision not to issue a notification under § 101(4), third sentence (§ 101(6), second sentence, point 1), and also the initial deferral of a notification under § 101(5), first sentence, require a court order (§ 101(6), second sentence, point 2) – may be dispensed with. The legislature had adopted these provisions in light of the transparency requirements set out by the Federal Constitutional Court in its judgement of 2 March 2010 – 1 BvR 256/08, BVerfGE 125, 260–385 – (see Bundestag document 18/5088, page 36). However, these provisions related to the retention of traffic and location data; such retention obligations are being removed from the law. Nor would it be appropriate for the notification requirements regarding the collection of traffic and usage data to be even stricter than those applicable to covert measures such as telecommunications interception under § 100a.

As explained above, for the sake of simplicity, sentence 2 will in future also apply to requests for identification data under § 100k(4) of the amended version. The following amendments therefore apply: To date, it has been possible to defer the notification pursuant to paragraph 7 sentence 2 in order to prevent the purpose of frustrating the information request. In future, pursuant to § 101a(4), second sentence, in conjunction with § 101(5), first sentence, notification must be given as soon as this is possible without jeopardising the purpose of the investigation, or the life, physical integrity or personal liberty of a person, or significant assets. The provision on non-disclosure set out in paragraph 7, sentence 3, is replaced by that in § 101(4), sentence 3, whereby, in future, notification may no longer be withheld solely on the grounds that it conflicts with the legitimate interests of third parties. The current § 101a(7), fourth sentence, which stipulates that the requirements set out in paragraph 4 must be logged, may be omitted, as this is in any case consistent with the principle of proper record-keeping.

As a result of the simplification described above (repeal of the special provision in § 101a(7) and reference to § 101(4)), the following changes apply to the collection of usage data under § 100k(4): A new feature is the reference in § 101a(4), second sentence, to § 101(4), second sentence, which requires a reference to subsequent legal remedies. Another new feature is the reference to § 101(4), fifth sentence, which stipulates that investigations to establish the identity of the person to be notified may only be carried out if this is necessary, taking into account the extent of the intrusion caused by the measure on that person, the effort involved in establishing their identity, and the resulting adverse effects on that person or others. Another new provision is that, under § 101(6), deferral of notification beyond 12 months is subject to judicial approval. Furthermore, legal protection will in future be governed by § 101(7), sentences 2 to 4, rather than, as has been the case to date, by § 98(2), sentence 2, applied by analogy, and § 304.

With regard to the collection of inventory data based on an IP address and in relation to specific data such as passwords under § 100j(2) and (3) of the amended version, the simplification (reference to § 101(4), sentences 2 to 5) has the same consequences as those described in relation to § 100k(4) in the previous paragraph. For the special notification requirement previously in force under § 100j(4) of the current version (see, regarding the constitutional background, Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 263; order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 246) is almost identical in wording to § 101a(7) of the current version.

No obligation to notify is introduced in respect of the preservation order under § 100g(7). Such an obligation would impose a considerable additional burden on the already heavily burdened law enforcement authorities. There is no need for this. This is because, when the secured data is collected, the notification requirement for data collection under § 100g(1) to (4) applies in any case; there appears to be no benefit in the data subject receiving two notifications. If the data is not collected and deleted, there is little reason to assume that anyone would be interested in being notified. For the purposes of transparency, however, a statistical obligation is introduced (see the amendment to § 101b). Since there is no obligation to notify under the first sentence, the reference in the second sentence to the second to fourth sentences of § 101(7), which provides for special legal protection arrangements, also does not apply. The preservation order is therefore governed by the recognised general rules on legal protection under § 98(2), second sentence, applied by analogy, and § 304.

Re Paragraph 5

This provision refers to § 100a(4) with regard to the duty of cooperation on the part of those required to provide information. § 100a(4) provides that any person who provides telecommunications services or is involved in such services must enable the court, the public prosecutor’s office and their investigative officers serving in the police force to carry out investigative measures and must provide the necessary information without delay. This reference already applies to telecommunications undertakings required to provide traffic data under the applicable law pursuant to paragraph 1 sentence 1 clause 1, to the providers of digital services required to provide usage data pursuant to paragraph 1a. A new addition to the list is the provision regarding access to subscriber data under § 100j, which telecommunications companies and digital service providers are also required to comply with. A provision comparable to § 100a(4) can be found in the current § 100j(5).

Re point 5 (§ 101b – Statistical recording; reporting obligations)

§ 101b sets out the requirements for the statistical recording of measures under § 100a et seq. – including § 100g and 100k – and the reporting obligations of the Länder and the Federal Public Prosecutor General arising therefrom. These standards are adjusted as follows:

Re (a)

This is an editorial amendment. It is not necessary to specify the section headings of § 100k at this point. The precise description of the measures to be included in the overviews is set out in paragraph 6.

Re (b)

Re (aa)

In paragraph 5(1), § 100g(1) to (4) and (7) are now listed individually. This means that requests for traffic data in relation to serious criminal offences (§ 100g(1)), criminal offences committed via telecommunications (§ 100g(2)), location data (§ 100g(3)) and cell site queries (§ 100g(4)) are recorded separately. This brings the structure of the information into line with that set out in § 100k, as under current law, measures under paragraph 1 (offences of significant importance) and paragraph 2 (offences committed via a telemedia or digital service) must already be presented separately.

Furthermore, the imposition of a preservation order is also subject to statistical reporting requirements (§ 100g(7)). This creates transparency about these measures even where data subjects are not notified of preservation orders (see the explanatory memorandum to §101a(4) sentence 1 above).

Re (bb)

This is a consequential amendment.

Re (c)

This is a follow-up amendment to the recast of § 100k. As before, the collection of usage data in relation to serious criminal offences (§ 100k(1)), criminal offences committed via digital services (§ 100k(2)) and location data (§ 100k(3)) is subject to reporting requirements. What is new is that the last group must be presented separately. This corresponds to the categories of data collection under § 100g.

Re Point 6 (§ 160a – Measures concerning persons bound by professional secrecy who are entitled to refuse to give evidence)

§ 160a sets out general provisions regarding measures applicable to persons bound by professional secrecy who are entitled to refuse to give evidence. Paragraph 5 currently states that § 100g(4) remains unaffected. As this provision is being deleted (see the explanatory notes to § 100g, prior to paragraph 1), this reference should be deleted as a consequential editorial amendment.

Article 2 (Amendment of the Introductory Act to the Code of Criminal Procedure)

The provision of § 12 is being revised. So far, the provision contains a transitional provision to the law introducing a storage obligation and a maximum storage period for traffic data, which has become obsolete.

In future, § 12 specifies the year for which the statistical reports are to be drawn up for the first time in the reporting year following the entry into force of the new version of § 101b(5) and (6). In the same year, the preservation order pursuant to § 100g(7) shall also be reported for the first time.

Re Article 3 (Amendment to the Electronic Evidence Implementation and Enforcement Act)

The amendments introduce the necessary provisions to make the European Preservation Order practicable under Regulation (EU) 2023/1543.

Re Point 1 (Table of contents)

This is an ancillary amendment to Point 2.

Re point 2 (§ 10a – Procedure for European Preservation Orders)

§ 10a clarifies Article 4(3) and (5) and Article 6 of Regulation (EU) 2023/1543. It lays down the conditions under which Member States may issue European Preservation Orders. It is clear from Article 4(3) that, unlike in the case of European Production Orders, European Preservation Orders do not distinguish between different categories of data. The provisions on the responsibilities set out in Article 4(3) therefore apply to all data categories.

It follows from Article 6(2) of Regulation (EU) 2023/1543 that European Preservation Orders must be intended to facilitate a subsequent request for production and must be necessary and proportionate for that purpose. In addition to a European Production Order, a European Investigation Order or other mutual legal assistance request can be selected for data production.

In addition, Article 6(3) distinguishes between European preservation orders issued for the purposes of criminal prosecution on the one hand, and for the purposes of the enforcement of sentences on the other: As with European production orders, the equivalence clause applies to law enforcement arrangements. This means that European preservation orders can only be issued in cases where protection is also possible under national regulations. In cases of the enforcement of sentences, however, the Regulation does not impose any such restriction and merely specifies, on the basis of the severity of the sentence or the nature of the measure, in which cases European preservation orders may be issued. This was decided at European level during the trilogue negotiations. In situations where there is already a final judgement, the person concerned should be regarded as less deserving of protection. Therefore, any existing restrictions of national law no longer apply at the stage of enforcement. The Regulation limits the differentiation thus made to the European Preservation Order; in the context of the European Production Order, the corresponding clause applies to both the prosecution and enforcement phases. The national legislature is bound by this.

Against this background, § 10a of the Act regulates the competence of the respective issuing authorities as follows:

Re Paragraph 1

Paragraph 1 provides that the competence of public prosecutor’s offices to issue European preservation orders for law enforcement purposes in accordance with Article 4(3)(a) of Regulation (EU) 2023/1543 is governed by the Eighth Section of the First Book of the Code of Criminal Procedure. This contains the legal bases for data security.

In view of the equivalence clause applicable to criminal proceedings under Article 6(3) of the Regulation (see above), the provisions of § 100g(7) of the Code of Criminal Procedure (new version) must be applied, under which a preservation order for traffic data may be issued. § 101a(1), first sentence, point 3(a) of the Code of Criminal Procedure further provides that, by way of derogation from § 100e(1), first to third sentences, of the Code of Criminal Procedure, the public prosecutor’s office is responsible for issuing such a

preservation order for the first three months. The power to issue such orders therefore lies initially with the public prosecutor's office alone. The security duration shall then be determined in accordance with Article 11(1) to (3) of Regulation (EU) 2023/1543. By way of derogation from national law, it is initially 60 days, renewable in accordance with the conditions laid down in the cited provision. Since the equivalence clause contained in Article 6(2) of the Regulation (see above) applies only to the imposition of the security measure, but not to its continuation, § 100e(1), fourth sentence, does not apply. No court order is therefore required to request an extension of the data retention period from the addressee on the basis of a European Preservation Order.

Re Paragraph 2

Paragraph 2 is based on Article 4(3)(b), and Article 4(5) of Regulation (EU) 2023/1543. Article 4(3)(b) complements the rule laid down in Article 4(3)(a), which lists the bodies primarily responsible for issuing preservation orders (see above). Point (b) provides Member States with the possibility to designate other authorities competent under national law to order the gathering of evidence in the relevant case. Within the framework of national regulations, these authorities may also issue European Preservation Orders; however, they must have them validated by a judge, a court, an investigating judge or a public prosecutor.

The Code of Criminal Procedure does not confer general authority to issue such orders on the bodies listed in paragraph 2, points 1 to 3, meaning that general authorisation under Article 4(3)(b) of the Regulation is not possible. However, pursuant to § 101a(1), first sentence, point 3(a) of the Code of Criminal Procedure (new version), the aforementioned authorities are authorised to issue a (national) preservation order in cases of imminent danger (alongside the public prosecutor's office; see the comments above regarding paragraph 1). For this emergency situation, designation in accordance with Article 4(5) in conjunction with Article 4(3)(b) of the Regulation is thus possible. However, further restrictive provisions of the Regulation must be observed, which, in Article 4(5), set out the procedure to be followed in the event of a 'justified emergency'. In particular this means: In a purely domestic case, a court must be involved only if – and only when – the measure is to be extended beyond three months (§ 101a(1), first sentence, point 3(a) of the Code of Criminal Procedure, as amended). By contrast, Article 4(5) of the Regulation also provides for validation in a 'reasoned emergency', which must be requested within 48 hours. Article 3(18) of the Regulation, to which Article 4(5) refers, defines a 'justified emergency' as 'a situation where there is an imminent threat to the life, physical integrity or safety of a person, or to critical infrastructure as defined in Article 2, point (a), of Directive 2008/114/EC, where the disruption or destruction of a critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including by seriously affecting the provision of basic services to the population or the exercise of the core functions of the State'. The definition of an urgent case is thus narrower in the Regulation than in national law, which allows for an order to be issued – for example by investigators from the public prosecutor's office – without the involvement of a judicial authority, provided there is an 'imminent danger' (of damage occurring or evidence being lost). Since the application of national law in cross-border cases is secondary to the Regulation, its conditions and procedures must be complied with. Although not provided for in national law, the entities referred to in points 1 to 3 of paragraph 2 must therefore request validation within 48 hours in the cross-border preservation order in the emergencies mentioned here.

Point 1 lists the investigating officers of the public prosecutor's office who, in domestic cases, may also issue preservation orders in cases of imminent danger in accordance with § 101a(1), first sentence, point 3(a) of the Code of Criminal Procedure (new version). In addition to police officers, this includes, in particular, tax authorities officials and customs administration officials in cases where they act as investigators for the public prosecutor's office by virtue of their legal assignment (e.g. § 404 of the German Fiscal

Code (AO), § 14 of the Act to Combat Undeclared Work and Unlawful Employment (SchwarzArbG), § 21 of the Foreign Trade and Payments Act, AWG).

Points 2 and 3 also authorise the tax- and customs administration authorities in situations where they are not acting as investigators for the public prosecutor's office, but are taking on that role by virtue of statutory provisions. This concerns the independent investigative powers of the tax authorities pursuant to § 399(1) and § 386(2) of the AO (e.g. in cases of exclusive tax offences) and the cases listed in § 14a and § 14b of the SchwarzArbG. The designation of these authorities as issuing authorities with merely secondary competence whose orders require additional validation by the public prosecutor's office in emergency situations, results from the wording of the Regulation (which refers to ‘public prosecutor's office’ in Article 4(1)(a)) and the case law of the European Court of Justice on the European Investigation Order (judgement of 2 March 2023, Case C-16/22) on the comparable question of interpretation.

Re Paragraph 3

Paragraph 3 sets out the procedure for ex-post validation. The Regulation does not regulate the ex post validation procedure, which is why it must be regulated in national law. Where an issuing authority has acted in an emergency pursuant to paragraph 2, it shall transmit the order referred to in the first sentence of paragraph 3 to the public prosecutor’s office within the period provided for in Article 4(5) of the Regulation (48 hours). This is done electronically using the transmission channel specified in Article 19(1) of the Regulation via the decentralised IT system to which all bodies involved in the issuing and validation process must be connected. The Public Prosecutor’s Office is reviewing the legality of the order issued in the light of the conditions set out in Regulation (EU) 2023/1543 (Article 4(3) and (5) and Article 5). In the case of ex-post validation, it records this in the files. The addressee will not be informed separately (see Annex II, Section F). In order to allow the issuing authority to immediately withdraw the order in case of refusal of ex-post validation (Article 4(5) of the Regulation), appropriate information on the refusal decision is required. Such a provision is to be integrated into the Guidelines for dealing with foreign countries in criminal matters (RiVASt).

Re Paragraph 4

Paragraph 4 provides for local jurisdiction for validation (substantive jurisdiction is determined by Paragraph 3). According to § 9(4), first sentence, the public prosecutor's office conducting the investigation is generally responsible for this, in accordance with its position as the authority in charge of the investigation; this may also be the Federal Prosecutor General. This ensures continuity in terms of content.

If, under national law, the secondary competent issuing authority conducts the investigations itself, the public prosecutor's office in whose regional court district the issuing authority is based is responsible.

The Federal States may adopt regulations that deviate from local jurisdiction, for example for reasons of specialisation.

Re Paragraph 5

Paragraph 5 sets out the rules on jurisdiction for the issuance of European preservation orders for the purposes of the enforcement of criminal sentences. Since the equivalence clause does not apply in this case due to the wording of Article 6(3) of Regulation (EU) 2023/1543 (see above), the requirements of national law do not automatically have to be complied with. However, in order to simplify the application of the law, it seems appropriate to ensure consistency with national competences. Paragraph 5 therefore designates the public prosecutor’s office as the competent authority. If the execution of

the sentence concerns juveniles or adolescents who have been sentenced to a youth sentence, the juvenile judge, as the enforcement officer, is competent to issue a preservation order. The latter also applies to the enforcement of housing in a psychiatric hospital and in a rehabilitation centres. This falls within the scope of the provisions of Article 4(3)(a) of the Regulation. Accordingly, both the courts and the public prosecutor's office have the power to act.

In addition, it is not possible to designate a secondary competent body. This is because the wording of Article 4(3)(b) of the Regulation expressly refers only to investigative authorities and the collection of evidence. This does not therefore cover situations relating to the enforcement of sentences.

Re Article 4 (Judicial Remuneration and Compensation Act)

The compensation scheme for information on inventory data for which traffic data must be used (point 201 of Annex 3 to the JVEG) will be adapted. Since the time required for this provision of information is comparable to that required for the provision of information under point 202 of Annex 3 to the JVEG, the amount of compensation should be adjusted accordingly. In return, the flat-rate fee will now only cover the retrieval of up to three identifiers, instead of the previous ten. In practice, this reduction is unlikely to have any effect, as law enforcement authorities regularly query only one identifier per request for information.

Points 309 to 311 of Annex 3 to the JVEG contain compensation for cable costs for the transmission of traffic data. The proposed Preliminary remark 3 is intended to ensure consistency with the rules on line costs related to the interception of telecommunications set out in § 1 of Annex 3 to the JVEG. Here, too, line costs should only be compensated if the line in question has been used at least once to transmit traffic data. It should also be made clear that the compensation is paid for the entire transmission period.

In addition, the JVEG will include compensation schemes for the services to be provided by telecommunications companies in connection with preservation orders.

The discount arrangement provided for in paragraph 2 of the General Preliminary Observations should also apply in the case of a preservation order. In addition, the headings of sections 3 and 4 should be amended.

The proposed new § 5 contains compensation schemes, in particular for the securing of traffic data by telecommunications companies. The grounds for compensation and the amounts payable are based on the corresponding provisions in Sections 3 and 4 concerning compensation for the provision of information without a prior preservation order.

For information on data stored by the telecommunications company on the basis of a previous preservation order, the new § 6 provides for compensation of EUR 20. It is assumed that, given the prior processing carried out in connection with the implementation of the preservation order, the effort involved in subsequently providing access to this data is generally relatively low. Account is taken of the increased costs which telecommunications undertakings may incur if, in individual cases, information is requested only in respect of a subset of the secured data.

Re Article 5 (Amendment to the Act on Administrative Offences)

This is a consequential amendment resulting from the amendment of § 100j of the Code of Criminal Procedure.

Re Article 6 (Amendment to the Telecommunications Act)

Re Point 1 (Table of contents)

The official table of contents shall be adapted in accordance with the changes made in point 2, as explained below.

Re point 2 (§ 175 to § 177)

The existing § 175 to § 181 are deleted without replacement. These are the existing, more far-reaching provisions on the general and indiscriminate retention of traffic and location data. They have been inapplicable since at least the ruling of the Federal Administrative Court of 14 August 2023 (6 C 6.22 and 6 C 7.22), which found them to be incompatible with EU law, and must therefore be repealed. § 175 to 177 are being revised and will in future contain provisions on the disclosure of traffic data to law enforcement and security authorities (§ 175), on the processing of traffic data pursuant to preservation orders (§ 176), and on the obligation to retain and the authority to use traffic data for the purpose of identifying subscribers (§ 177).

Regarding § 175 (Authority to process traffic data for the purpose of providing information to law enforcement and security authorities)

§ 175 serves to clarify the legal position and provide legal certainty for the telecommunications services concerned with regard to the power to process traffic data for the purpose of providing information to certain authorised bodies. A corresponding provision expressly authorising the telecommunications companies concerned to process traffic data for the purpose of providing information on traffic data is currently not in place in the TKG, although the legal bases for access rights and collection powers with regard to traffic data exist for the bodies referred to in paragraph 3. However, according to the case law of the Federal Constitutional Court on the constitutional requirements for the ‘double-door’ model (Federal Constitutional Court, decision of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph), in addition to the legal basis of the authorities entitling them to request information and collect data, there must also be the authority of the telecommunications companies responsible for data processing to process the data for the purpose of providing information (the ‘double-door’ model).

Re Paragraph 1

Paragraph 1 clarifies that the undertakings concerned shall be authorised to process traffic data for the purpose of providing information where the bodies referred to in paragraph 3 request them to provide information on traffic data with reference to the aforementioned legal bases and submit the relevant order for that purpose. The same applies to companies or other network operators which a provider uses as upstream providers to process traffic data on its behalf for the provision of its telecommunications services.

Re Paragraph 2

In accordance with paragraph 2, the undertakings concerned must comply with the formal requirements set out therein when receiving requests for information. The requesting authorities are solely responsible for ensuring that the request for information and the collection of this traffic data are lawful.

Re Paragraph 3

Paragraph 3 authorises the undertakings concerned to provide information on traffic data, as referred to in the first sentence of paragraph 1, solely to the bodies listed in points 1 to 9; in this context, the undertakings are unable to verify the substantive legal requirements for disclosure for practical reasons and are therefore not required to do so. Their examination shall be limited to compliance with the formal requirements referred to in paragraph 2.

Through the provisions on data transfer set out in paragraph 3, the federal legislature is, rather, fulfilling its constitutional duty to regulate by ensuring that, when opening up the data holdings of private companies for use in the performance of state functions (change of purpose), it simultaneously defines the amended purposes of use and the essential conditions for such use (see Federal Constitutional Court, decision of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 130 et seq.).

Paragraph 2 authorises the disclosure of traffic data to the security authorities of the federal states, insofar as this is necessary in individual cases to avert a specific threat to a legal interest of at least considerable importance or to avert a specific threat to public safety. In order to avert a specific danger, there must at least be factual indications that a specific danger to the interests protected is emerging (see Federal Constitutional Court, judgement of 1 October 2024 – 1 BvR 1160/19 – BVerfGE 141, 220–378, paragraph 111 et seq.).

Paragraph 7 authorises the disclosure of communications data to the state offices for the protection of the constitution, subject to the conditions set out therein, for the purpose of fulfilling the intelligence-gathering mandate of the offices for the protection of the constitution, which derives either from § 3(1) of the Federal Act on the Protection of the Constitution or from the respective state acts on the protection of the constitution. This applies in particular to the protection of the constitutional order against the aspirations and activities of organised crime.

Re Paragraph 4

With reference to the obligation of confidentiality pursuant to the second sentence of § 174(6), the undertakings providing information shall, in the interests of the statutory performance of their tasks by the requesting authorities, respect the confidentiality of such information.

Paragraph 4 also refers to the obligation to apply the provisions on the electronic procedure for providing information, as well as on data security and data protection, set out in § 174(7). These regulations therefore ensure that there are established and standardised procedures for dealing with requests for information from public authorities. These procedures enable the organisations concerned to process requests for information efficiently and provide the authorised bodies with a standardised, technical procedure for submitting such requests.

Regarding § 176 (Authority to process traffic data for the purpose of complying with preservation orders)

§ 176 grants providers the power to process traffic data in connection with the implementation of preservation orders pursuant to § 100g(7) of the Code of Criminal Procedure, § 10b(1) or § 52(3) of the Federal Criminal Police Office Act, and § 25a(1) of the Federal Police Act, as well as in response to requests for information based on these provisions. In addition, an obligation to implement appropriate data protection and data security measures is regulated.

Re Paragraph 1

Paragraph 1 authorises, on the one hand, providers who are the addressees of a preservation order under § 100g(7) of the Code of Criminal Procedure, or under § 10b(1) or § 52(3) of the Federal Criminal Police Office Act, and under § 25a(1) of the Federal Police Act, to carry out the necessary processing of traffic data generated by the use of the service, as well as traffic data to be generated in the future (§ 3(70)). The same applies to companies or other network operators which a provider uses as upstream providers to process traffic data on its behalf for the provision of its telecommunications services. In doing so, the telecommunications service provider must also ensure the immediate preservation of data which it has not itself generated and processed in the course of the provision of its service. The provider must demonstrate to the Federal Network Agency, at the Agency's request, how it ensures this security. By virtue of the second sentence, the power to process data also covers the response to subsequent requests for information from the secured traffic data to the authorised bodies under the conditions laid down in Paragraph 175.

Secured data may only be disclosed in response to a request for information that directly corresponds to the preservation order. Authorisation to access data is determined by the jurisdiction responsible for the underlying proceedings. If, for example, the preservation order has been issued by the Federal Criminal Police Office acting as the central authority, and the Federal Criminal Police Office has in the meantime transferred the proceedings to a state public prosecutor's office prior to the data being retrieved, then from the time of transfer only that public prosecutor's office is authorised to retrieve the data. The prerequisite is always that the proceedings in question are the same (although it is not detrimental if, for example, the charge changes in the course of the proceedings). Consequently, public authorities whose requests for data are unrelated to the prior preservation order are therefore precluded from collecting preserved data.

The Telecommunications Act regulates only the powers relating to data processing for the purpose of providing information. The obligation to transfer data to authorised entities arises from the legal bases of the authorised entities or from the relevant order. Specific details regarding data retention, in particular concerning the recipients, the data required and the retention period, are set out in the relevant preservation order issued by the ordering authority.

Furthermore, paragraph 1 clarifies that such data, in so far as they have been secured solely on the basis of a preservation order, may not be used for any other purpose. The term 'solely' makes it clear that the processing of such traffic data – which is also stored by telecommunications providers subject to the obligation for other reasons – is not restricted by a preservation order. This applies in particular to data that obliged entities store for operational reasons and have additionally secured on the basis of a preservation order relating to the same data. As long as the data is still stored for operational reasons, it may, for example, also be processed in response to requests for information received in the meantime from other authorities.

Re Paragraph 2

Paragraph 2 requires the addressees referred to in the first sentence of paragraph 1 to ensure compliance with data protection and data security requirements.

Pursuant to paragraph 1, obliged entities must ensure that data secured on the basis of preservation orders are protected against unauthorised access and use by means of state-of-the-art technical and organisational measures.

Paragraph 2 stipulates that traffic data must be stored in a manner that is technically separate from all other end-user data held by the data controller, using a secure and

reliable data processing system. The criterion of ‘technical’ stems from the judgement of the Court of Justice of the European Union of 30 April 2024 (Case C-470/21, Quadrature du Net II – Hadopi, paragraphs 87 and 164), which requires, from a technical perspective, an effective and strict separation between the various categories of data retained. This decision relates directly to IP addresses that have been stored as a precautionary measure. However, it stands to reason that these requirements should also apply to data that has been stored pursuant to a preservation order. This is because these are not merely data that enable the identification of a subscriber, but also include further traffic or location data, which are often of a more sensitive nature.

In accordance with paragraph 3, the provider must store data in such a way that requests for disclosure from the relevant authorities can be complied with without delay.

Point 4 contains an obligation to delete data secured by a preservation order immediately after the ordered data transmission to the issuing body has taken place. The data shall be deleted to the extent that they have been accessed. Where the addressees of a preservation order have not been requested to disclose data, or have not been requested to do so in full, they must immediately, and at the latest upon expiry of the time limit specified in the preservation order, irreversibly delete such data in accordance with the state of the art and, in particular, the provisions of the Technical Guidelines, or ensure that such irreversible deletion takes place.

In this context, the term ‘without delay’ as defined in § 121(1), first sentence, of the Civil Code means that an action must be taken without culpable delay, but not necessarily immediately. The key point is that, with careful organisation and attention, the person involved could not have reacted any faster, although unavoidable obstacles may prolong the time taken.

The immediate irreversible deletion of a data record after the expiry of the respective storage period can take place in a multi-stage procedure, which is described by the technical guideline according to § 170(6). This takes into account the fact that in most cases the secure deletion of individual files is only possible to a limited extent according to the state of the art, for example according to the CON.6 ‘Delete and destroy’ module of the Federal Office for Information Security.

Nevertheless, the requirements now laid down for the protection of data to be secured deliberately fall short of the standards for data protection and security set out in the general and indiscriminate data retention scheme – which has been declared permanently inapplicable. The strict rules on data protection and data security in § 176 to 181 resulted from the direct implementation of the judgement of the Federal Constitutional Court, which declared the first German data retention scheme unconstitutional (judgement of 2 March 2010 – 1 BvR 256/08, BVerfGE 125, 260-385). Apart from the aforementioned provisions, they do not have to be reproduced for the preservation order, as no permanently existing data pool with corresponding risks of misuse is provided for in this respect. Unlike data retention, data storage under a preservation order is carried out on an ad hoc basis, in individual cases, for a limited period of time and only in respect of a limited scope of data. Furthermore, it is not publicly known whether data is stored, to what extent, or concerning whom. The traffic data stored on the basis of a preservation order is therefore a much less attractive target for potential external attacks. Under the legislation currently in force, in particular the Telecommunications Act (TKG) and the Telecommunications Data Retention Act (TDDDG), provisions on data protection and data security are in place for traffic data stored for operational purposes; these provisions will apply – in addition to the requirements set out in paragraph 2 – to data stored pursuant to the data preservation order.

Re Paragraph 3

Those subject to a preservation order under paragraph 1, first sentence, must maintain confidentiality regarding the existence of such an order, any subsequent preservation order issued in connection therewith, and any data transfer carried out on that basis, in the interests of the requesting authorities' lawful performance of their duties.

Re Paragraph 4

The provisions of the Act laid down in paragraphs 2 and 3 require further specification. The Federal Government is therefore authorised to issue detailed regulations on data security and data protection, as well as on the procedure for providing information, in the statutory instrument pursuant to § 170(5) of the Telecommunications Interception Ordinance (TKÜV), which provides the basis for the proper implementation of the regulations. The Federal Network Agency sets out the technical details for this in the Technical Guideline pursuant to § 170(6).

The provisions governing the design of protective measures and data erasure, as well as the procedure for providing information and for complying with the confidentiality requirement in accordance with the provisions of the TKÜV and the Technical Guideline pursuant to § 170(6) continue the provisions previously applicable to the provision of information on traffic data and thus guarantee established and standardised procedures for dealing with preservation orders and requests for information.

These procedures enable obliged providers to efficiently process preservation orders and requests for information, as well as a standardised, technical procedure for transmission of the preservation order and requests for information for the authorised bodies. The TKÜV already sets out, amongst other things, organisational requirements regarding technical acceptance and the provision of assistance outside business hours. The TKÜV also contains regulations on security requirements for information requests, which are extended to include the obligations under paragraph 2 in order to ensure a uniform level of security.

The measures taken shall be notified to the Federal Network Agency. The Federal Network Agency reviews the implementation of the requirements approximately every two years.

Regarding § 177 (Obligation to retain and power to use traffic data for the purpose of identifying subscribers)

The regulation sets out requirements for internet service providers regarding the retention of IP addresses for a period of three months and the identification of additional data required – such as port numbers – to enable these addresses to be unambiguously linked to a subscriber, as well as the authorised use of such data.

Such a data retention obligation is consistent with constitutional law. This data retention obligation is considerably less burdensome than the full retention of data relating to all telecommunications connections and may therefore be ordered by law under significantly less stringent conditions (see Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260–385, paragraph 257; order of 27 May 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238, paragraph 171). There is a heightened interest – recognised under constitutional law – in the possibility of attributing internet communications to specific parties in order to protect legal interests or uphold the rule of law. Given the obvious importance of the internet for a wide variety of areas and processes in everyday life, there is also a constant risk that it may be used to commit a wide range of criminal offences. In a state governed by the rule of law, the internet must not be allowed to become a legal vacuum. In order to ensure the reliable allocation of IP

addresses to subscribers over a certain period of time, the legislator may therefore provide for the relevant data to be retained by service providers (see Federal Constitutional Court, judgement of 2 March 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, paragraph 260).

The data retention obligation is also consistent with EU law, specifically with Article 15(1) of 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), as interpreted in the light of Articles 7, 8 and 11, and Article 52(1) of the Charter of Fundamental Rights of the European Union. The storage ordered here does not constitute a serious infringement of these rights, as the storage arrangements ensure that its scope is limited solely to identifying a subscriber associated with a known IP address; it is impossible to track the websites visited by a subscriber or to identify their contacts or locations (see the relevant guidelines of the Court of Justice of the European Union, judgement of 30 April 2024, Case C-470/21, Quadrature du Net II – Hadopi, paragraphs 101 and 115).

Re Paragraph 1

Paragraph 1 lays down an obligation to store IP addresses and supplementary necessary data, such as port numbers and time stamps at the source of a connection with the provider of an internet access service, solely for the purpose of identifying the subscriber and for a limited period of three months. The provision is technology-neutral in order to take into account the various procedures for awarding IP addresses.

Only providers of internet access services are obliged to do so (see § 3(23)). The same applies to companies or other network operators which a provider uses as upstream providers to process the traffic data for the provision of its internet access service. In so doing, internet access service providers must also ensure the immediate preservation of data which it does not generate and process itself in the course of the provision of its service. The provider must demonstrate to the Federal Network Agency, at the Agency's request, how it ensures this security.

Number-independent interpersonal telecommunications services (OTT-1 services, such as messaging and email services) are therefore not required to retain data for precautionary purposes. Providers of local wireless networks (such as a hotel operator providing Wi-Fi to its guests or an initiative allowing the temporary sharing of private local networks) also do not belong to the circle of obliged entities. According to Article 2(2)(2) of Regulation (EU) 2015/2120, to which Paragraph 3(23) refers, internet access service is 'a publicly available electronic communications service which provides access to the internet and thus connections to virtually all internet termination points, irrespective of the network technology and terminal equipment used'. However, local wireless networks do not themselves provide access 'to the internet and thus connections to virtually all of the internet's endpoints'; rather, they merely provide – figuratively speaking – a route to it. For their part, they depend on a connection to an internet access service and its telecommunications service. Only these entities provide actual 'access to the Internet' (i.e. to Internet nodes or the networks of other ISPs). Accordingly, the local wireless networks do not assign a public Internet protocol address, but only network/router-internal IP addresses. Furthermore, Freifunk associations are not subject to the obligation set out in paragraph 1, as they do not assign a telephone number or connection identifier – i.e. a public IP address – to either the owner of the Freifunk router or the Freifunk user. From the user's perspective, the provision of the service is similar to sharing a room in a hotel, where no registration is required and an IP address is assigned to a device. The service is always based on an internet access service provided by another internet service provider who is themselves subject to the obligations set out in paragraph 1.

Given the current state of technology, the service provider is always able to provide the requested information if the law enforcement agency's request includes the IP address, port number and timestamp relating to the connection. Paragraph 1 requires the storage of the public IP address; the port number and, where applicable, other traffic data referred to in paragraph 2 are generally only required for the identification of the subscriber if the same public IP address is assigned to several users via a specific technical procedure (Network Address Translation, NAT). However, the investigating authorities often do not have the port number to hand, so they contact the provider using only the IP address and timestamp. In this case, the provider is obliged to provide the information, even in the absence of a port number, provided that this is technically feasible. In this case, it may be possible to clearly link the connection to a specific subscriber if the provider has exclusively assigned an IP address to the subscriber for the underlying connection, meaning that it is not necessary to distinguish between connections using a port number. See also the explanatory memorandum to the amendment to the Code of Criminal Procedure, point 3, regarding § 100j(2).

In accordance with paragraph 3, the internet access provider must store a unique identifier for the connection and an assigned user ID. In this context, the connection identifier refers to the network operator's physical access point at the subscriber's premises, as also covered by § 172(1), first sentence, point 2. In the case of internet access services, these are typically the identifiers of lines permanently assigned to the Internet connection. The assigned user identifier shall mean the identifier provided by the internet access service provider to the subscriber for authentication against the network of the internet access service provider. This identifier is regularly registered on the internet router (e.g. DSL modem) of the subscriber and is used to log in to the login server of the internet access provider. In any event, the data retention system must be technically designed in such a way as to ensure that subscribers can be identified and information about them provided throughout the retention period (see, in this regard, the requirements set out in the decision of the Federal Constitutional Court of 20 December 2018 – 2 BvR 2377/16 – and the decision of the Federal Court of Justice of 28 April 2021 – StB 47/20).

The date and time (to the nearest second) to be recorded in accordance with point 4 should refer not only to the start and end of the allocation of public IP addresses, but also to the start and end of the allocation of a port number, where this is required under point 2. Finally, within the period of allocation of an IP address, different port numbers may be successively assigned to that IP address. If only the period of allocation for the IP address were stored, several subscribers would also be eligible if the same port number was assigned to each subscriber in the total period. Only by also recording the time period during which the port number was assigned can a subscriber be identified with certainty.

The obliged entity continuously stores all necessary data, from the beginning, over the duration of the connection, up to and including the end of the connection. Any data that exceeds the retention period during this connection will be deleted on an ongoing basis, including the initial data if it falls outside the three-month retention period. The start of the three-month retention period serves as the new 'notional' starting point. This means that no data is stored for longer than three months, yet the ability to identify subscribers is guaranteed throughout the retention period.

In sentence 2, the retention period is set at three months. It complies with the requirement set out by the Court of Justice of the European Union in its judgement of 30 April 2024 (Case C-470/21, Quadrature du Net II – Hadopi, paragraph 93), according to which the duration of storage must be limited to what is strictly necessary.

In the case of crimes committed on or via the Internet, the IP address of the perpetrator is often the only, but always the first, most efficient and fastest investigation approach for law enforcement or investigative authorities. In the field of intelligence gathering, too, access to IP addresses is a relevant and often essential tool. Without assignment of the IP

address to a connection owner, investigations and knowledge gathering often run into the sand unless there are other clues.

The necessary duration of storage depends, in particular, on the point in time at which the security authority becomes aware of the IP addresses relevant to the offence. Only then can the investigative and security authorities use the IP address to submit a request to the internet service provider for subscriber details relating to the customer's connection. This varies from case to case and also depends on the nature of the crime; it depends on how quickly the investigating authority becomes aware of a criminal offence or a potentially dangerous situation – and of a potentially relevant IP address – through, for example, a criminal complaint from the public, a report from digital service providers, a request or tip-off from abroad, or data from seized storage media. In some cases, more recent contributions to the crime must also be clarified.

In the case of the dissemination of child pornography, it has been shown that electronic evidence uncovered and seized during a search may contain IP addresses of possible accomplices, which may already be several weeks and months old. Even in cases of commercial extortion using ransomware, evaluation of affected systems and existing log data can be complex and therefore time-intensive. If a German IP address relevant to the offence is identified in the process, it may be impossible to link it to the offender's connection because the digital trace extracted is older. In cases of international cooperation concerning crimes against children and young people, it is not uncommon for several months to have already passed by the time information relevant to the investigation reaches the Federal Criminal Police Office. In investigations into organised and commercial drug-related crime, service providers are asked to supply the login details of accomplices who can only be uniquely identified by the IP address used. If these are older than a few days, case files cannot be referred to the locally competent law enforcement authority.

In the case of threat processing in the area of terrorism, relevant IP addresses may already be several months old at the time of receipt of notice of attack plans. In cases involving intelligence operations and state-sponsored terrorism, IP addresses can also be used to identify the connection from which the perpetrator logged into networks or sent an email, thereby enabling targeted investigations. As with the phenomenon of (cyber) espionage, it must be assumed that these involve long-term activities by foreign intelligence services, and the periods in question are generally longer and often date back some time. Such cases often only become known to the security authorities after several months of delay.

When it comes to hate speech, there are cases in which IP addresses dating back several months may still be relevant to the investigation. Victims of online fraud often do not realise they have been targeted until several weeks have passed. Even communications from abroad about cybergrooming by a German Internet user sometimes only become known after several weeks have elapsed.

An IP address must therefore be associated with a connection for at least that period. For example, it provides added value in many areas of phenomena for the purposes of law enforcement and police and intelligence activities. For this period, in view of victims of crimes committed online and the dangers posed by political extremism and terrorism, as well as the threats posed by espionage activities, it must be ensured that the security authorities are able to determine the connection used by the perpetrator in order to investigate the offence.

Practical police experience shows that a storage period of three months is likely to cover a relevant part of the significant police facts. When determining the necessary retention period, the success rates achieved to date by the BKA – that is, the proportion of cases in which the BKA, in its capacity as central office, was able to determine local jurisdiction by

querying the database – cannot be applied generally to the individually standardised NCMEC process. It is a highly optimised and, in particular, automated process which makes it possible to drastically reduce the time taken to obtain inventory data on the basis of an IP address. The NCMEC process involves platform providers in the US being required to report depictions of sexual violence that they discover during voluntary searches to the National Center for Missing & Exploited Children (NCMEC), which in turn forwards such information to the BKA – the German Federal Criminal Police Office – for the purposes of criminal prosecution. Under the NCMEC process, service providers (via NCMEC) provide standardised data relevant to criminal proceedings, together with evidence. The technical process established here cannot be applied to investigations in other areas of crime, where, due to the nature of the offences, IP addresses relevant to the case are sometimes only brought to the attention of the police at a later stage in the proceedings, or must first be identified through measures that are time-consuming and resource-intensive. The storage period of three months is therefore necessary, but also sufficient to ensure the availability of the relevant data in many configurations. The three-month storage period thus brings the urgent need of the competent law enforcement authorities to effectively investigate criminal offences and ward off dangers into appropriate balance with fundamental rights, especially those of innocent citizens affected by storage.

Sentence 3 clarifies that the content of communications, as well as data relating to visits to websites or the use of other telecommunications or digital services – that is, the destination IP addresses of a communication – may not be stored under this provision.

Re Paragraph 2

Paragraph 2 provides that those providers of internet access services which, in the provision of their service, make use of undertakings or other network operators as ‘providers’ and therefore do not themselves process all traffic data, are subject to further obligations. In this case, providers of internet access services shall also ensure the immediate storage of the data not produced and processed by them themselves during the provision of their service. Suppliers must provide evidence to the Federal Network Agency, upon request, of the measures they have taken to ensure storage.

Re Paragraph 3

Paragraph 3 requires the addressees referred to in the first sentence of paragraph 1 to ensure compliance with data protection and data security requirements.

In accordance with paragraph 1, those subject to the obligations set out in that paragraph must ensure that the data to be stored pursuant to paragraph 1 is protected against unauthorised access and use by means of state-of-the-art technical and organisational measures.

With regard to the procedures for data retention, the Court of Justice of the European Union set out various requirements in its judgement of 30 April 2024 (Case C-470/21, Quadrature du Net II – Hadopi). Under that provision, the retained data referred to in paragraph 1 must in any event be technically effectively separated from any other end-user data held by the obliged entity by a secured and reliable data processing facility, which is transposed by point 2. The implementation of this requirement is then to be carried out by regular inspection by an independent body and is ensured in paragraph 5 by the Federal Network Agency.

Point 3 stipulates that the data to be secured on the basis of paragraph 1 must be stored in such a way that the information can be provided to the authorised bodies without delay, as is also the case under point 3 of § 176(2). Which bodies are authorised to do so follows

indirectly from paragraph 4, which specifies the purposes for which stored data may be used.

Paragraph 4 stipulates that data required to be stored under paragraph 1 must be deleted after three months. In the event that a law enforcement authority from another European country issues a European preservation order on the basis of Regulation (EU) 2023/1543 for the preparation of a subsequent production order to acquire subscriber data, the obliged entity shall ensure that they comply with any subsequent production order, i.e. can provide access to subscriber data, for example by separating the data or preparing access to subscriber data.

The requirements regarding the protection of data to be stored are deliberately less stringent than the provisions on protection and security set out in § 176 to 181 – as is the case under § 176(2) for the reasons described therein.

Re Paragraph 4

Paragraph 4 contains the purpose limitation provision, which exhaustively sets out the purposes for which data stored as a precautionary measure under paragraph 1 may be used. Accordingly, the data may be used, firstly, to provide information in accordance with § 174(1), third sentence; § 174(5) specifies to which bodies information may be disclosed and under what conditions. This includes, in particular, the law enforcement and security authorities, but also the intelligence services designated there. The data referred to in paragraph 1 may also be used to comply with a European Production Order for the purpose of obtaining subscriber data in accordance with Regulation (EU) 2023/1543, i.e. where a law enforcement authority of another Member State requests information from a German internet access service provider or issues a European Preservation Order in preparation for such a request. Data may not be used for any other purposes. In particular, it is not permissible to disclose data pursuant to a European Production Order for the purpose of obtaining traffic data.

Sentence 1 further provides that an efficient technical procedure is to be used which does not impair separate storage as per paragraph (2) number 2. For information pursuant to § 174(1), third sentence, the third sentence refers to the procedure pursuant to § 174(7) for obtaining information from subscribers. It uses a secure electronic interface for 100 000 and more contractual partners as well as the email-based transmission procedure, which must also be used by all other obligated parties. The secure electronic interface uses a method that has been in place for years and is widely regarded as a reliable means of providing information. The interface is based on an ETSI standard (TS 102 657), which guarantees a uniform approach on both sides to parties to proceedings. The standardised processes for handling requests for information and for providing responses ensure that these are dealt with promptly and to a consistently high standard on both sides. It reduces the frequency of errors to a minimum, is future-proof through the uniform standard and is available on the free market. The common standard and the machine-readable format used allow for partial automation on the part of obligated entities, which can facilitate the compilation of requested data and speed up the provision of information. Authorised bodies can quickly and easily import large volumes of enquiries into the system using pre-formatted files, and processed enquiries can be easily organised and analysed using custom filters.

Re Paragraph 5

The provisions of the Act set out in paragraph 3 require further elaboration – as is the case with § 176(4) in relation to § 176(2). The Federal Government is therefore authorised to issue detailed regulations regarding the obligations set out in paragraph 3, including specifications concerning the systems, procedures and technical equipment used to store

the data referred to in paragraph 1 of the TKÜV, which provides the basis for the proper implementation of the regulations.

The protective measures taken shall be submitted to the Federal Network Agency. The Federal Network Agency reviews the implementation of the requirements approximately every two years.

Re point 3 (§ 228 – provisions on fines)

The amendments are consequential editorial amendments which are necessary as a result of the amendment of § 175 to 177 and the deletion of the previous § 177 to 181.

To ensure the practical effectiveness of § 174(6), first sentence, this provision – which imposes a duty on the telecommunications companies concerned to disclose information – must be enforceable by means of a fine. This also helps to avoid the inconsistency in the legal framework that would otherwise arise if maintaining confidentiality were punishable by a fine, whereas the actual obligation to disclose information were not.

Re point 4 (§ 230 – Transitional provisions)

The provision regulates from when the storage obligation of traffic data for the identification of subscribers pursuant to § 177 applies.

Re Article 7 (Amendment to the Telecommunications Interception Ordinance)

These are consequential amendments to individual provisions of § 2, 32 and 35 of the Ordinance which are necessary as a result of the amendment of § 175 to 177 of the Telecommunications Act and the deletion of the current § 177 to 181 of the Telecommunications Act. The changes are editorial in nature.

Re Article 8 (Amendment to the Telecommunications Digital Services Act – Data Protection Act)

§ 13a (Fulfilment of obligations under Articles 10 and 11 of Regulation (EU) 2023/1543)

§ 13a was inserted into the TDDDG as part of the implementation of Regulation (EU) 2023/1543 (Federal Law Gazette 2026 I No. 64). The provision ensures that providers of electronic telecommunications services subject to European Preservation and Production Orders are permitted to process the requested data in order to comply with those orders.

The new § 176(2) of the Telecommunications Act lays down data protection and data security requirements in connection with the national preservation order regulated therein. Given the similarity of the circumstances, these requirements should apply mutatis mutandis to preservation orders issued under Regulation (EU) 2023/1543 (unless already provided for in the Regulation). To this end, a new paragraph 2 is added to § 13a. This does not entail any additional costs for the providers concerned, as they already have the necessary technical and organisational arrangements in place under § 176(2) of the Telecommunications Act.

Re Article 9 (Amendment to the Federal Police Act)

Re Point 1 (Table of contents)

This is a consequential editorial amendment.

Re Point 2 (§ 25 – Collection of traffic and usage data)

Re (a)

In the first sentence of paragraph 1, reference is made to the legal definition in § 3(70) of the Telecommunications Act in order to clarify the meaning of the term ‘traffic data’.

Re (b)

The insertion ‘when backing up data from a radio cell’ has been newly inserted. This clarifies that the second clause – which states that a description of the telecommunications that is sufficiently specific in terms of time and place is sufficient, provided that otherwise achieving the purpose of the measure would be futile or significantly impeded – applies in cases where data from a mobile phone cell is being secured.

Re (c)

Reference is made to the justification for point 2(b).

Re (d)

Paragraph 6 is amended by the insertion of the second sentence, which clarifies that the question of whether and to what extent arrangements must be made to fulfil the obligation to cooperate under the first sentence is governed by the Telecommunications Act (TKG) and the Telecommunications Interception Ordinance (TKÜV). This provision is consistent with the structure of comparable obligations to cooperate, for example in the case of telecommunications interception under § 40(8), second sentence, of the Federal Police Act, as set out in the draft bill on the modernisation of the Federal Police Act (Bundestag Paper 21/3051) for the Federal Police, and in § 51(6), second sentence, of the Federal Criminal Police Office Act (BKAG) for the Federal Criminal Police Office.

Re point 3 (§ 25a – Retention of traffic data)

§ 25a is newly inserted. It introduces the instrument of a preservation order relating to traffic data for the Federal Police.

The scenarios falling within the remit of the Federal Police relate to cases involving (sometimes life-threatening) smuggling of people in containers, the entry of extremists or terrorists, and terrorist attacks on airports, ports or railway facilities.

Intelligence agencies regularly receive reports of planned smuggling operations, the entry of extremists or terrorists, and attacks on airports, railway facilities and ports. In the context of this information, individual German telephone numbers can often be mentioned. However, at this stage, the evidence does not yet allow the police officers involved to identify specific individual rogue actors. The Federal Police need to carry out further investigative work to consolidate the information, in the course of which suspicions will be substantiated, rogue actors identified and links between individuals established. However, these further investigations are time-intensive, especially in the context of organised crime and often difficult-to-see personal networks, especially if the references are limited to individual phone numbers. In such cases, it is essential for the successful prevention of danger that the traffic data of those individuals for whom there are actual grounds to believe that collection will be permissible at a later date be secured before the conditions for collecting such data have been met.

Within the scope of its competence, the Federal Police has currently issued alerts in the Schengen Information System for more than 40000 persons with links to extremism or

terrorism for the purpose of refusing entry. There is regular evidence to suggest that these entry refusals are being circumvented by unauthorised entries. In this context, as is often the case at the beginning of such dangerous situations, only a mobile phone number is known to the authorities, which could be associated with the intended entry of an extremist-motivated group with links to organised crime. It is of the utmost importance that the traffic data relating to this mobile phone number can be secured as quickly as possible under the terms of the preservation order, so that it can be retrieved retrospectively at a later date.

Re Paragraph 1

Paragraph 1 lays down the substantive conditions for the preservation order. It states that a preservation order may be issued in respect of a person who has a personal or geographical connection to the danger or the offence to be prevented under § 25(1) of the Federal Police Act, as set out in the draft Act on the Modernisation of the Federal Police Act (Bundestag document 21/3051), and where there are factual indications that the person is a person within the meaning of § 25(1) and that an investigation under § 25(1) might be justified, or where there are factual indications that the person is a person who is connected to a person under § 25(1)(2) or (3) in a manner that is not merely fleeting or incidental and in a way that justifies the assumption that, following the acquisition of further information, an investigation under § 25(1) might be justified.

The preservation order is designed to meet the Federal Police's need to secure ephemeral data when the available evidence and information do not yet allow for sufficiently specific identification of individual individuals posing a threat or causing disruption. In order to be permitted to collect communications data in such cases, it is first necessary to further consolidate the information, a process which serves to substantiate grounds for suspicion, identify potential threats or disruptive individuals, and clarify links between people.

At the start of the risk assessment, it is often the case that there is not yet enough information available to attribute the risk to a specific threat or disruptive element. Furthermore, the nature of the relationships with a rogue actor's communication partners is usually not entirely clear. Only if this becomes clear in the course of the investigation of the facts is it permissible to collect data on the persons referred to in § 25(1). Until that date, it should be ensured that relevant traffic data is not erased.

The same applies to telecommunications devices identified as belonging to individuals associated with the perpetrator, or to potential locations where the perpetrator and their contacts may be staying or operating (including the preservation of highly volatile mobile phone cell data), until it has been determined whether a traffic data collection order may be issued in respect of them pursuant to § 52(1). In that case, the targeted and complete collection of traffic data can be carried out by the court.

The mechanism of the preservation order also takes account of the fact that, in certain circumstances, where the conditions for the collection of traffic data are met, an order to preserve such data must be issued at the same time in order to prevent data loss. Please refer to the comments on § 100g(7) of the Code of Criminal Procedure.

The traffic data must be relevant for the purposes specified in § 25(1). Unlike with collection, it is therefore not necessary that averting the danger or preventing the aforementioned offences would otherwise be futile or significantly impeded. Rather, it is sufficient if, on the basis of an ex-ante forecast, it is to be expected that the secured traffic data will be required for security measures under § 25(1).

Re Paragraph 2

Paragraph 2 sets out who is authorised to order the security measure. The content, form and time limit of the order are largely identical to the requirements for an order for the collection of traffic and usage data pursuant to § 25(5). By way of derogation from § 25(5), the order is issued not by the court, but by the authority authorised to issue the order. The content of the order is regulated by way of derogation from § 25(5) in so far as, in the case of a preservation order, the nature of the data to be collected by the measure and their foreseeable significance for the purpose of collection must also be indicated. It is further provided that the court shall decide on the extension of the preservation order upon application by the person authorised to make such an order under the first sentence.

Re Paragraph 3

Paragraph 3 provides that the obligated party on the basis of a preservation order pursuant to paragraph 1 shall immediately and fully secure the data covered by the order. Furthermore, with regard to the question of whether and to what extent measures need to be taken in this respect, reference is made to the corresponding application of § 25(6), second sentence, to the provisions of the Telecommunications Act (TKG) and the Telecommunications Interception Ordinance (TKÜV). In addition, the reference to § 25(7) extends the obligation to compensate the parties obligated to provide information on traffic and usage data to the parties obligated to protect traffic data.

Re Article 10 (Amendment to the Law on Associations)

Re Point 1

To date, § 4(4), first sentence, refers to § 94 to § 97, § 98(4) and § 99 to § 101 of the Code of Criminal Procedure. The reference therefore also includes the newly inserted § 100a et seq. of the Code of Criminal Procedure. The provisions on the interception of telecommunications contained therein are not applicable to the seizure of objects in the investigation procedure under the Vereinsgesetz (Law on Associations) and are therefore to be excluded from the referral.

Re Point 2

The current § 4(4), fourth sentence, also refers to § 105(4) of the Code of Criminal Procedure. The paragraph referred to has since been repealed; the reference must be amended accordingly.

§ 111c, § 111n to § 111p of the Code of Criminal Procedure have been added to the list of references. They concern provisions relating to the manner of seizure, surrender, the relevant procedural rules and the emergency sale. These provisions will also apply mutatis mutandis to the seizure of property under the Associations Act.

Re Article 11 (Amendment to the Money Laundering Act)

Under the current § 29(2a), second sentence, point 2, the Central Office for Financial Transaction Investigations may not process data under § 100k(1), second sentence, of the Code of Criminal Procedure using automated data analysis procedures. The exclusion therefore only applies to existing (retrograde) location data collected from digital services, but not to other usage data.

Under the new regulatory framework, the collection of traffic data in relation to telecommunications services under § 100g of the Code of Criminal Procedure and the collection of usage data under § 100k of the Code of Criminal Procedure are treated largely in the same way. Such a distinction is also inappropriate under the Money Laundering Act and is therefore repealed. In future, this means that all data obtained

through an investigation under § 100k of the Code of Criminal Procedure will be excluded from processing in automated data analysis systems.

Re Article 12 (Restriction of a fundamental right)

The provision complies with the requirement to cite the relevant legal basis, as the fundamental right under Article 10 of the Basic Law is restricted by the amended provisions of the Code of Criminal Procedure in Article 1(2) and (3), the Telecommunications Act in Article 6(2) and the Federal Police Act in Article 9(3).

Re Article 13 (Entry into force)

This provision provides for entry into force.