

Draft Act

of the Federal Government

Draft of an Act transposing Directive (EU) 2023/1544 and implementing 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

A. Problem and objective

The draft is intended firstly to transpose Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down uniform rules on the assignment of designated establishments and the appointment of representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181). Secondly, it serves to implement 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 (OJ L 191, 28.7.2023, p. 118). The two dossiers were negotiated in the bodies of the European Union under the heading 'e-evidence'. In particular, the European regulations are a response to the rapidly growing importance of digital media in the initiation and execution of criminal acts. They make it possible for law executing authorities in EU Member States to order the preservation and production of certain personal data across borders under certain conditions.

The new parent act, which implements the e-evidence mechanism into German law, is a response to the rapidly growing importance of digital media in the initiation and execution of criminal acts. The act creates a uniform legal framework and ensures that the e-evidence-specific provisions are practical and user-friendly. The aim is to increase the efficiency of law enforcement in the Federal Republic of Germany and in the European Union.

This draft is in line with the objectives of the UN General Assembly resolution of 25 September 2015 'Transforming our world: the 2030 Agenda for Sustainable Development', the timely achievement of which is now at risk. The draft contributes to the achievement of Objectives 16.a and 16.6, supporting the fight against crime and building effective institutions at all levels.

B. Solution

The provisions of Directive (EU) 2023/1544 and the implementing provisions of Regulation (EU) 2023/1543 will be standardised in a new parent act. This will be structured into four parts:

- The general provisions lay down determinations that are applicable to the parent act as a whole.
- The provisions transposing Directive (EU) 2023/1544 introduce the European requirements into national law.

- Regulation (EU) 2023/1543 is embedded in the existing German regulatory framework with implementing provisions.
- The administrative fine penalises infringements committed by service providers in violation of their obligations under the parent act as well as Regulation (EU) 2023/1543.

As national legislation currently contains obligations for service providers that go beyond the content of Article 1(4) of Directive (EU) 2023/1544, the provision in the Telecommunications Act (TKG) on the appointment of authorised representatives for receipt or delivery is declared inapplicable within the scope of this Directive.

The Telecommunications Digital Services Data Protection Act (TDDDG) is supplemented by the power to process data for service providers on the basis of European preservation and production orders.

C. Alternatives

None.

D. Budget expenditure excluding compliance costs

When the law comes into force in 2026, the Federal Government will incur one-off personnel costs estimated at EUR 1 216 000.

The ongoing annual personnel costs are estimated to be EUR 741 000 from 2027 onwards.

The additional material and staffing requirements will be compensated for in individual plan 07 in terms of funds and jobs.

The Federal States will incur additional personnel costs totalling around EUR 273 000.

E. Compliance costs

E.1 Compliance costs for citizens

Citizens will not incur any compliance costs.

E.2 Compliance costs for businesses

For businesses, this will result in an increase in annual compliance costs amounting to about EUR 126 000. This will result in a one-off expenditure of around EUR 1.3 million.

Administrative costs under this heading arising from information duties

Of which, around EUR 123 000 is attributable to administrative costs arising from obligations to provide information.

E.3 Compliance costs for the authorities

The authorities will incur one-off compliance costs of EUR 948 000 in 2026. These costs will be incurred exclusively at federal level.

The annual compliance costs amount to around EUR 816 000. Of this amount, EUR 257 000 is attributable to the state level (including municipalities); at the federal level, the costs amount to around EUR 559 000.

F. Other costs

For these provisions, the effects on the burden and relief for the issuing authorities under §§ 9 and 10 as well as the effects on the burden on the competent local courts and higher regional courts must be taken into account by the legal protection provisions in §§ 13 to 17, as well as the activity of the public prosecutor's offices as executing authorities pursuant to § 18(2).

As Regulation (EU) 2023/1543 simplifies the procedures for obtaining the necessary data, fewer authorities will need to be involved in future. This will result in an estimated reduction in costs of EUR 2.7 million for the Federal Republic of Germany.

Draft Act of the Federal Government

Draft of an Act transposing Directive (EU) 2023/1544 and implementing 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 proceedings¹

of ...

The Federal Parliament has adopted the following Act:

Article 1

Act on European Production Orders and Preservation Orders on Electronic Evidence

(Electronic Evidence Implementation and Enforcement Act – EBewMG)

Table of Contents

Part 1

General regulations

§ 1 Definitions

Part 2

Transposition of Directive (EU) 2023/1544

§ 2 Sector of application

§ 3 Designated establishments and representatives (addressees)

§ 4 Notifications and languages

§ 5 Joint responsibility of service providers and addressees

§ 6 Central authority

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);

Article 1(1) to (6), and Article 18(1), (3)(1)(a), (7)(1), and Articles 2 and 3 of this Act are intended firstly to transpose Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down uniform rules on the assignment of designated establishments and the appointment of representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181).

Part 3
Implementation of Regulation (EU) 2023/1543

Chapter 1
General provisions

§ 7 Applicability of other procedural and jurisdictional provisions

Chapter 2
European production orders and preservation orders

§ 8 Data categories for outgoing orders

§ 9 Procedure for European production orders concerning subscriber data and identification data

§ 10 Procedure for European production orders for traffic data and content data

§ 11 Competent executing authority

§ 12 Statistical obligations

Chapter 3
Judicial protection

Section 1
Appeals against outgoing orders

§ 13 Applicable provisions

§ 14 Judicial decision

Section 2
Procedure for conflicting obligations

§ 15 Judicial proceedings

§ 16 Judicial decision

Section 3
Appeals against decisions in enforcement proceedings

§ 17 Application of the Administrative Offences Act

Part 4
Provisions on fines and restriction of a fundamental right

§ 18 Provisions on fines

§ 19 Restriction of a fundamental right

Teil 1

General regulations

§ 1

Definitions

The definitions in Article 2 of Directive (EU) 2023/1544, as amended on 12 July 2023, and Article 3 of Regulation (EU) 2023/1543, as amended on 12 July 2023, apply to this Act. The term 'addressee' is used as defined by Article 7(1) of Regulation (EU) 2023/1543, as amended on 12 July 2023.

Teil 2

Transposition of Directive (EU) 2023/1544

§ 2

Sector of application

(1) This part applies to orders and decisions to collect electronic evidence in criminal proceedings on the basis of

1. Regulation (EU) 2023/1543, in the version of 12 July 2023;
2. Directive 2014/41/EU, as amended on 13 December 2023;
3. the Convention of 29 May 2000, drawn up by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (BGBl. [Federal Law Gazette] 2005 II p. 650, 651) and
4. national law, where the order or decision is addressed to a natural person or legal entity acting as a representative or designated establishment of a service provider in the territory of the Federal Republic of Germany.

(2) This part is without prejudice to the powers of the German investigative authorities to contact the service providers established in the territory of the Federal Republic of Germany directly in accordance with European Union law and national law on the collection of electronic evidence in criminal proceedings.

§ 3

Designated establishments and representatives (addressees)

(1) Service providers with one or more establishments in the territory of the Federal Republic of Germany and in other Member States of the European Union applying the legal instruments referred to in § 2(1) shall designate at least one of these establishments as the addressee in accordance with Paragraphs 4 and 5. Upon designation, a location

must be chosen where the service provider offers its services. If the service provider has establishments exclusively in Member States as defined by Sentence 1 in which it does not offer services, one of these establishments must be designated as the addressee in accordance with Paragraphs 4 and 5. The addressee is responsible for the receipt, compliance and enforcement of decisions and orders that fall within the scope of § 2(1).

(2) Service providers with one or more establishments exclusively within the territory of the Federal Republic of Germany shall, in accordance with Paragraphs 4 and 5, designate at least one of these establishments as the addressee as defined by Paragraph 1(4), if they offer their services within the territory of the Federal Republic of Germany and additionally or alternatively in another Member State of the European Union.

(3) Service providers who offer their services in the territory of the Federal Republic of Germany but do not have an establishment there or in a Member State of the European Union that applies the legal instruments referred to in § 2(1) shall appoint at least one representative as addressee as defined by Paragraph 1(4), in accordance with Paragraphs 4 and 5, in the territory of the Federal Republic of Germany or in a Member State of the European Union that applies the legal instruments referred to in § 2(1) and in which they offer their services.

(4) Service providers that are established or that offer services in the territory of the Federal Republic of Germany must provide their addressees with the authorisations and resources necessary to comply with decisions and orders issued by a Member State of the European Union that fall within the scope of application specified in § 2(1).

(5) Service providers that offer services in the European Union as of 18 February 2026 are required to designate or appoint at least one addressee in accordance with Paragraphs 1 to 3 by 18 August 2026. Service providers who begin offering services in the European Union after 18 February 2026 are required to designate or appoint at least one addressee in accordance with Paragraphs 1 to 3 within six months of the date on which they began offering services in the European Union.

(6) Addressees of service providers that are established or that offer services in the territory of the Federal Republic of Germany are obliged to cooperate with the competent authorities in accordance with the applicable statutory provisions when receiving decisions and orders pursuant to § 2(1).

§ 4

Notifications and languages

(1) Service providers whose addressees are based in the territory of the Federal Republic of Germany are required to provide the Federal Office of Justice with the contact details of these addressees and any changes thereto in writing, in accordance with Paragraphs 3 to 5.

(2) Service providers who have designated or appointed their addressees in other Member States of the European Union and

1. are established in the territory of the Federal Republic of Germany without offering services there, or
2. that offer their services in the territory of the Federal Republic of Germany

are required, in accordance with Article 6(1) of Directive (EU) 2023/1544, as amended on 12 July 2023, to provide the contact details of these addressees and all other relevant information to the central authorities designated by the respective Member States of the European Union in accordance with Paragraphs 3 to 5.

(3) Service providers must specify the exact geographical scope in their communications when designating or ordering

1. several addressees in the territory of the Federal Republic of Germany,
2. one or more addressees in other Member States of the European Union in addition to one or more addressees in the territory of the Federal Republic of Germany,
3. several addressees only in other Member States of the European Union.

(4) In their communications, service providers must indicate which official language or languages of the European Union may be used in correspondence with the addressee or addressees. If the addressee is based in Germany, these languages must include German.

(5) The notifications must be made immediately after expiry of the relevant deadline specified in § 3(5) or, in the case of any changes, immediately after they occur.

§ 5

Joint responsibility of service providers and addressees

(1) Both the service provider and the addressee shall be responsible for the non-fulfilment of obligations arising from decisions and orders falling within the scope of § 2(1). This shall apply regardless of which of the two committed the act or omission constituting the breach of duty, and even if there are no appropriate internal procedures in place between the service provider and the addressee.

(2) The joint liability pursuant to Paragraph 1 shall not apply if the act or omission constituting the breach of duty is a criminal offence in the territory of the Federal Republic of Germany.

§ 6

Central authority

(1) As the central authority, the Federal Office of Justice monitors compliance with the obligations arising for service providers and their addressees from §§ 3 and 4 within the territory of the Federal Republic of Germany. The Federal Office of Justice may collect and process the data necessary to fulfil the task referred to in Sentence 1, including personal data. In addition, the Federal Office of Justice may request information and evidence from addressees located within German territory, in particular regarding the powers and resources available to addressees pursuant to § 3(4).

(2) In order to fulfil its tasks pursuant to Paragraph 1, the Federal Office of Justice shall cooperate and coordinate with the central authorities of other Member States of the European Union and, where necessary, with the European Commission. In doing so, the Federal Office of Justice shall support the central authorities of the other Member States

of the European Union by providing all appropriate information and administrative assistance.

(3) The Federal Office of Justice shall immediately forward the information received in accordance with § 4 and any related updates to the European Judicial Network in criminal matters upon receipt from the service providers so that it can be published on its publicly accessible website. In addition, the Federal Office of Justice shall publish the information on its own website.

(4) The Federal Office of Justice shall inform the Commission annually of the service providers that have failed to 1 comply with their obligations under §§ 3 and 4, which enforcement measures have been taken against them and which penalties have been imposed on them.

Teil 3

Implementation of Regulation (EU) 2023/1543

Kapitel 1

General provisions

§ 7

Applicability of other procedural and jurisdictional provisions

Insofar as Regulation (EU) 2023/1543 as amended on 12 July 2023 and the following provisions of Part III of this Act do not provide for special procedural and jurisdictional provisions, the provisions of the Courts Constitution Act (GVG), the Introductory Act to the Courts Constitution Act, the Code of Criminal Procedure (StPO), the Youth Courts Act (JGG), the Fiscal Code (AO) and the Act to Combat Undeclared Work and Unlawful Employment (SchwarzArbG) shall apply.

Kapitel 2

European production and preservation orders

§ 8

Data categories for outgoing orders

(1) Subscriber data as defined by Article 3(9) of Regulation (EU) 2023/1543, as amended on 12 July 2023, includes in particular

1. Inventory data pursuant to § 3(6) and data pursuant to § 172 of the Telecommunications Act,

2. Inventory data pursuant to § 2(2)(2) of the Telecommunications Digital Services Data Protection Act.

(2) Data requested solely for the purpose of identifying the user as defined by Article 3(10) of Regulation (EU) 2023/1543 as amended on 12 July 2023 includes, in particular, usage data pursuant to § 2(2)(3)(a) of the Telecommunications Digital Services Data Protection Act.

(3) Traffic data as defined by Article 3(11) of Regulation (EU) 2023/1543, as amended on 12 July 2023, includes in particular

1. Traffic data pursuant to § 3(70) of the Telecommunications Act;
2. Usage data pursuant to § 2(2)(3)(b) and (c) of the Telecommunications Digital Services Data Protection Act.

§ 9

Procedure for European production orders concerning subscriber data and identification data

(1) The jurisdiction of the courts and public prosecutor's offices to issue European production orders for the purpose of obtaining subscriber data or data requested for the sole purpose of identifying the user pursuant to Article 4(1)(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) Insofar as they are authorised to take criminal proceedings under national law, the following authorities are responsible for issuing European production orders to obtain subscriber data or data requested solely for the purpose of identifying the user, in accordance with Article 4(1)(b) of Regulation (EU) 2023/1543, as amended on 12 July 2023:

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 forward the European production order to the public prosecutor's office for validation. In the case of validation, the public prosecutor's office shall forward the European production order to the addressee. The decision regarding validation and the transmission of the certificate to the addressee shall be recorded in the 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 adopt different provisions for local jurisdiction.

(5) If, under national law, the courts have jurisdiction to issue orders, the procedure shall be governed by § 10(2) and (3).

§ 10

Procedure for European production orders for traffic data and content data

(1) The jurisdiction of the courts to issue European production orders for the purpose of obtaining traffic data, with the exception of data requested solely for the purpose of identifying the user, or for obtaining content data pursuant to Article 4(2)(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) Before public prosecution is instituted, the European production order is issued at the request of the investigating public prosecutor's office or, in cases where the tax authorities or customs authorities conduct the investigations independently under national law, at their request. The provisions of § 162(1)(1) and (3) and § 169 of the Code of Criminal Procedure, Section III of Part VIII of the Fiscal Code and Section IV of the Act to Combat Undeclared Work and Unlawful Employment shall apply accordingly.

(3) When issuing the European production order, the court shall forward the certificate to the addressee. If one of the authorities referred to in Paragraph 2(1) has requested the issuance of a European production order and, after judicial review, the conditions for this are not met, the court shall reject the request. §§ 304 and 306 of the Code of Criminal Procedure shall apply accordingly to appeals against the rejection decision. The issue of the European production order and the transmission of the corresponding certificate or the rejection of the request shall be recorded in the file.

§ 11

Competent executing authority

(1) The executing authority, as defined by Article 3(17) of Regulation (EU) 2023/1543, as amended on 12 July 2023, is the public prosecutor's office. The public prosecutor's office at the regional court in whose district the addressee of the order resides or has his registered office has local jurisdiction. The Federal States may adopt different provisions for local jurisdiction.

(2) If the issuing authority of another Member State of the European Union contacts a domestic authority that does not have jurisdiction, the request must be forwarded immediately to the competent authority in accordance with Paragraph 1 and the issuing authority must be informed of the competent authority.

§ 12

Statistical obligations

(1) Within their area of competence, the judicial administrations of the Federal States and the Federal Prosecutor General collect the data referred to in Article 28(2) of Regulation (EU) 2023/1543, as amended on 12 July 2023, and transmit them to the Federal Office of Justice by 28 February of the year following the reporting year each calendar year.

(2) The Federal Office of Justice shall compile an overview of the data referred to in Paragraph 1 and shall forward the overview to the European Commission by 31 March of the year following the reporting year at the latest.

Kapitel 3

Judicial protection

Section 1

Appeals against outgoing orders

§ 13

Applicable provisions

(1) § 98(2)(2), § 304(1) and §§ 306 and 310(2) of the Code of Criminal Procedure shall apply accordingly to appeals against European production orders requesting subscriber data. The same applies to European production orders issued by the public prosecutor's office to collect data for the sole purpose of identifying the user.

(2) For appeals against European production orders requesting traffic data, § 101a(6)(2) in conjunction with § 101(7)(2) and § 311 of the Code of Criminal Procedure shall apply accordingly. The same shall apply to court-ordered European production orders to collect data for the sole purpose of identifying the user.

(3) For appeals against European production orders requesting content data, § 95a(5)(1) and (2), § 101(7)(2) and (3), § 304(1), §§ 306, 310(2) and § 311 of the Code of Criminal Procedure shall apply accordingly.

(4) The remedies referred to in Paragraphs 1 to 3 shall only be available to persons whose data has been requested by means of a European production order pursuant to Regulation (EU) 2023/1543, as amended on 12 July 2023.

§ 14

Judicial decision

(1) In the case of European production orders, the court shall examine whether the conditions for issuance pursuant to Article 4(1), (2), (4) and (5) and Article 5 of Regulation (EU) 2023/1543, as amended on 12 July 2023, have been met.

(2) If the conditions have not been met, the court shall declare the European production order unlawful and shall revoke it.

Section 2

Procedure for conflicting obligations

§ 15

Judicial proceedings

(1) The issuing authority's application for a court ruling in the event of conflicting obligations pursuant to Article 17(3)(2) of Regulation (EU) 2023/1543 as amended on 12 July 2023 may be appealed before the ordinary courts.

(2) The Higher Regional Court shall decide on the application of the issuing authority under Paragraph 1. The Higher Regional Court in whose district the issuing authority has its seat shall have local jurisdiction. Notwithstanding Sentence 1, the Federal Court of Justice shall decide in cases where the order was issued by the Federal Prosecutor General or the investigating judge of the Federal Court of Justice.

(3) The issuing authority shall attach to the request the outcome of its examination of the reasoned objection and any comments made by the executing state in accordance with Article 17(3)(1) of Regulation (EU) 2023/1543, as amended on 12 July 2023.

(4) §§ 42 and 43(2) of the Code of Criminal Procedure shall apply accordingly to the calculation of the time limit pursuant to Article 17(2)(3) of Regulation (EU) 2023/1543, as amended on 12 July 2023.

§ 16

Judicial decision

The decision of the Higher Regional Court or the Federal Court of Justice pursuant to Article 17(5) or (8) of Regulation (EU) 2023/1543, as amended on 12 July 2023, shall be made by way of an order from which no appeal lies.

Section 3

Appeals against decisions in enforcement proceedings

§ 17

Application of the Administrative Offences Act

Appeals against decisions in enforcement proceedings pursuant to Article 16(10)(2) of Regulation (EU) 2023/1543, as amended on 12 July 2023, shall be governed by the provisions of Section Five of Part Two of the Administrative Offences Act.

Teil 4

Provisions on fines and restriction of a fundamental right

§ 18

Provisions on fines

(1) A regulatory offence shall be deemed to have been committed by any person who, intentionally or negligently:

1. contrary to § 3(1)(1)(2) or (3) or § 3(2), fails to designate an establishment specified therein, fails to do so correctly or in good time;
2. contrary to § 3(3), fails to appoint a responsible representative, or fails to do so correctly or in good time; or
3. contrary to § 4(1) or (2), fails to submit a notification, or fails to do so correctly, in full or in good time.

(2) A contravention of Regulation (EU) 2023/1543, as amended on 12 July 2023, is deemed to have been committed by anyone who, intentionally or negligently:

1. contrary to Article 10(1) or (2)(2) fails to act, fails to act correctly or in good time;
2. contrary to Article 10(2)(1) fails to ensure that requested data is transmitted;
3. contrary to Article 10(3), fails to ensure that requested data is transmitted;
4. contrary to Article 10(4)(1) fails to transmit requested data or fails to do so in good time,
5. contrary to Article 10(6)(1)(1), (7)(1) or (8)(1) or Article 11(5)(1), (6)(1) or (7)(1), fails to inform an authority referred to therein, or fails to do so correctly or in good time;
6. contrary to Article 10(6)(1)(2) fails to submit a notification, or fails to do so correctly, in full or in good time;
7. contrary to Article 10(6)(2)(2) or Article 11(5)(2), fails to ensure that he or she can obtain the clarification or correction referred to therein;
8. contrary to Article 11(1)(1) in conjunction with Sentence 2, fails to secure the requested data, or fails to do so in good time or for the prescribed period;
9. contravenes an enforceable order pursuant to Article 11(1)(3)
10. fails to secure data requested pursuant to Article 11(2) or fails to secure it for the prescribed period; or
11. contrary to Article 13(4), fails to take a measure specified therein, or fails to do so correctly or in full.

(3) The regulatory offence may be punished

1. in cases referred to in
 - a) Paragraph 1 and
 - b) Paragraph 2(1) to (4) and (7) to (11)by a fine of up to five hundred thousand euro and
2. in cases referred to in Paragraph 2(5) and (6), by a fine of up to up to one hundred thousand euros.

(4) By way of derogation from Paragraph 3(1)(b), for a service provider with a total turnover of more than EUR 25 million, including in conjunction with § 30(2)(2), of the Administrative Offences Act, an administrative offence under Paragraph 2(1) to (4) and (7) to (11) may be punishable by a fine of up to 2% of the total turnover.

(5) By way of derogation from Paragraph 3(2), for a service provider with a total turnover of more than EUR 5 million, including in conjunction with § 30(2)(2), of the Administrative Offences Act, an administrative offence under Paragraph 2(5) or (6) may be punishable by a fine of up to 2% of the total turnover.

(6) Total turnover for the purposes of Paragraphs 4 and 5 is the sum of all sales revenue generated worldwide by the service provider in the financial year preceding the public authority's decision. The total turnover may be estimated.

(7) § 17(2) of the Administrative Offences Act shall not apply to the imposition of a fine on a service provider in the cases referred to in Paragraph 2.

(8) The administrative authority as defined in § 36(1)(1) of the Administrative Offences Act is

1. in the cases referred to in Paragraph 1, the Federal Office of Justice;
2. in the cases referred to in Paragraph 2, the executing authority referred to in § 11(1).

§ 19

Restriction of a fundamental right

Secrecy of communications (Article 10(1) of the Basic Law) shall be restricted in accordance with this Act.

Article 2

Amendment to the Telecommunications Act

The Telecommunications Act of 23 June 2021 (BGBl. I p. 1858), last amended by Article 1 of the Act of 24 July 2025 (BGBl. 2025 I, No 181), is amended as follows:

After § 170(11), the following Paragraph 12 is inserted:

(1) ‘ The provisions of Paragraph 1(3)(b) and Paragraph 2(2)(c) shall not apply within the scope of Directive (EU) 2023/1544, as amended on 12 July 2023.’

Article 3

Amendment of the Telecommunications Digital Services Data Protection Act

The Telecommunications Digital Services Data Protection Act (TDDDG) of 23 June 2021 (BGBl. I p. 1982; 2022 I p. 1045), as last amended by Article 44 of the Law of 12 July 2024 (BGBl. 2024 I, No 234), is amended as follows:

1. The table of contents is changed as follows:

a) The following wording is inserted after the wording relating to § 13:

‘§ 13a Compliance with obligations pursuant to Articles 10 and 11 of Regulation (EU) 2023/1543, as amended on 12 July 2023’.

b) The following wording is inserted after the wording relating to § 24:

‘§ 24a Compliance with obligations pursuant to Articles 10 and 11 of Regulation (EU) 2023/1543, as amended on 12 July 2023’.

2. After § 13, the following § 13a is inserted:

‘§ 13a

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

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.’

3. After § 24, the following § 24a is inserted:

‘§ 24a

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

Providers of digital services and the addressees established by them in accordance with § 3(1) to (3) of the Electronic Evidence Implementation and Enforcement Act may 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.

Article 4

Entry into force

(1) This Act shall enter into force on the day after its promulgation, subject to Paragraph 2.

(2) On 18 August 2026, the following shall enter into force:

1. In Article , §§ 7 to 17, § 18(2), (3)(1)(b) and (2), §§ 4 to 7 and § 8(2) and § 19 of the Electronic Evidence Implementation and Enforcement Act and
2. Article 3.

EU legal acts:

1. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1; L 143 of 9 June 2015, p. 16), as last amended by Directive (EU) 2023/2843 of 13 December 2023 (OJ L, 2023/2843, 27 December 2023)
2. 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)
3. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down uniform rules on the assignment of designated establishments and the appointment of representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181)

Justification

A. General part

I. Objectives and necessity of the regulations

The Act is intended firstly to transpose Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down uniform rules on the assignment of establishments and the appointment of representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181; in the following: Directive (EU) 2023/1544). Secondly, the Act serves to implement 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; in the following: Regulation (EU) 2023/1543).

The law is in line with the objectives of the United Nations General Assembly resolution of 25 September 2015, 'Transforming our world: the 2030 Agenda for Sustainable Development', the timely achievement of which is now at risk. The draft contributes to the achievement of Objectives 16.a and 16.6, supporting the fight against crime and building effective institutions at all levels.

1. Directive (EU) 2023/1544

Article 7(1) of Directive (EU) 2023/1544 requires Member States to adopt the laws, regulations and administrative provisions necessary to comply with the Directive by 18 February 2026 at the latest.

The aim of the Directive is to establish uniform rules for the representation of certain service providers in the European Union. This is to ensure that decisions by the competent authorities of the Member States to collect electronic evidence in criminal proceedings can be received, complied with and enforced.

To achieve this, a new parent act will be introduced with the Electronic Evidence Implementation and Enforcement Act. In addition, amendments to the Telecommunications Act and the Telecommunications and Telecommunications Telemedia Data Protection Act are necessary.

2. Regulation (EU) 2023/1543

Regulation (EU) 2023/1543 shall apply from 18 August 2026 in all Member States of the European Union with the exception of Denmark, which, in accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the TEU and the TFEU, did not participate in the adoption of the Regulation and is neither bound by it nor obliged to apply it. As directly applicable Union law, the Regulation does not require transposition in the Federal Republic of Germany. However, in the interests of ensuring that the Regulation is applied seamlessly and, in conjunction with national law, as clearly as possible, individual implementing provisions are necessary.

The aim of Regulation (EU) 2023/1543 is to create a new legal framework for the collection of electronic evidence across border. The authorities of a Member State may have such evidence secured or requested directly from a service provider who has designated an establishment or appointed a representative in another Member State of the European Union, regardless of where the data is located (Article 1(1) of the Regulation). Pursuant to Article 1(2) of Regulation (EU) 2023/1543, a European production order or a European preservation order may also be requested by the accused or their defence counsel within the framework of the applicable rights of defence, if and to the extent that this is provided for in national criminal procedure law. The Code of Criminal Procedure (StPO) provides for corresponding provisions in § 136(1)(3) and § 166 for preliminary and interim proceedings, as well as in § 244(3) to (6) for criminal proceedings.

In order to implement Regulation (EU) 2023/1543, specific provisions are set out in the newly introduced Electronic Evidence Implementation and Enforcement Act. These provisions relate in particular to responsibilities and procedures for the orders provided for in the Regulation. Legal protection is also provided for.

Further provisions, for example on how executing authorities should deal with incoming orders and decisions, may be included in the Guidelines on Relations with Foreign Countries in Criminal Matters (RiVAST) in order to facilitate the application of the Regulation and the Directive in legal practice.

II. Origin of the legal acts

Regulation (EU) 2023/1543 and the accompanying Directive (EU) 2023/1544 respond to the sharp increase in the cross-border use of electronic communications and digital services in the preparation and execution of criminal acts. This poses particular challenges for law executing authorities. On the one hand, data required as electronic evidence may be located in the territory of other Member States, and on the other hand, traditional methods of investigative cooperation often prove too cumbersome in view of the dynamic and decentralised storage locations in the digital space.

Not least in the wake of the terrorist attacks in Brussels on 22 March 2016, the Member States of the European Union called on the European Commission in the conclusions of the Council of the European Union of 9 June 2016 to develop a common approach for the European Union, in particular to speed up mutual legal assistance procedures and cooperation with service providers. The European Parliament addressed this issue in its resolution on combating cybercrime of 3 October 2017. It emphasised that fragmented legal frameworks can be a problem for service providers seeking to comply with requests from law executing authorities. The European Parliament therefore called on the European Commission to present a proposal for a European Union legal framework for electronic evidence with sufficient safeguards for the rights and freedoms of all those concerned.

On 17 April 2018, the European Commission then submitted a draft package consisting of a regulation and a directive to the Council of the European Union and the European Parliament, based on Article 82(1) (for the regulation) and Articles 53 and 62 of the Treaty on the Functioning of the European Union (for the directive). The core concept behind the legal instruments is to break through the mechanism of administrative cooperation in 'traditional' mutual legal assistance and to empower and enable investigating authorities to issue orders for data preservation or production directly to service providers in another Member State of the European Union.

Negotiations on the package of measures began in April 2018 in the COPEN Council Working Party. In December 2018, the Council of the European Union (Justice and Home Affairs) reached a general agreement on large parts of the text of the regulation (see Council document 15104/17 COPEN 380 of 8 December 2016). The Federal Republic of Germany did not agree with the general approach and issued a protocol statement after failing to enforce a clear and transparent anchoring of fundamental rights. After a pandemic-related pause, trilogue negotiations between the European Commission, the European Parliament and the Council of the European Union began in early 2021, resulting in a compromise that was deemed acceptable by the Federal Republic of Germany. The regulation agreed on a relatively robust notification procedure and specific provisions for the protection of data held by those bound by professional secrecy. The Federal Republic of Germany therefore had no objections when the Council reached its final decision on 27 June 2023. However, it issued a statement for the minutes indicating that, within the framework of the information procedure, the grounds for rejection protecting individual rights must be examined, which is not sufficiently clear in the recitals of the Regulation. From the point of view of the rule of law, it is also essential that legal protection exists not only against production orders and in the issuing state, but also against preservation orders and in the executing state.

The Regulation and the Directive are published in the Official Journal of the European Union (OJ L 191/118 of 28 July 2023, L 191/181 of 28 July 2023). The Regulation will apply in the Member States of the European Union from 18 August 2026, and the Directive must be transposed by 18 February 2026.

III. Main content of the legal acts

1. Regulation (EU) 2023/1543

The Regulation establishes a European production order and a European preservation order, which can be used to secure and obtain electronic evidence directly from the service providers concerned across borders (Article 1(1) of the Regulation).

The decisive factor in determining whether a case is cross-border is not the location where the data in question is processed, but the location of the addressee that is acting on behalf of the service provider in question (Article 3(1) of the Regulation). All service providers operating within the European Union are subject to the obligations under the Regulation (Article 2(1) of the Regulation). The scope of application covers subscriber, traffic and content data (Articles 4, 5 and 6 in conjunction with Article 3(8) to (12) of the Regulation); real-time collection is not provided for. The orders may be issued in the context of and for criminal proceedings and for the enforcement of custodial sentences or measures involving deprivation of liberty with a minimum duration of four months (Article 2(2) of the Regulation).

In terms of procedure, the Regulation first distinguishes between orders for preservation (Article 6) and orders for production (Article 5). With regard to the production order, a further distinction is made: Is it directed at subscriber data and traffic data that serve solely for identification purposes ('identification data') or at content and (other) traffic data? Since the former data categories are considered less sensitive, less stringent requirements for orders are to be observed (Article 4(1), Article 5(3) of the Regulation). The same applies to preservation orders (with regard to all data categories, Article 4(3) and Article 6 of the Regulation). In all cases, the investigating authority of the state wishing to issue an order must assess the proportionality of the measure (Article 5(2) and Article 6(2) of the Regulation). While the public prosecutor's office may order the preservation and production of subscriber and identification data for all criminal offences (Article 4(1) and (3), Article 5(3) and Article 6(3) of the Regulation), the production of traffic and content data can only be ordered by a court in connection with offences for

which a minimum maximum penalty of three years applies, or for certain categories of offences (e.g. in the area of sexual abuse of children or terrorism) (Article 4(2), Article 5(4) of the Regulation). A further condition for production and preservation orders is that a similar order could be issued in a comparable national case under the same conditions (Article 5(2) and Article 6(3) of the Regulation). Production orders must always be addressed to the service provider acting as the controller as defined by Regulation (EU) 2016/679 (Article 5(6) of Regulation (EU) 2023/1543). If data held by a service provider for a public authority is affected, a European production order may only be issued if the public authority concerned is located in the issuing state (Article 5(8) of the Regulation). This is to prevent the investigating authorities of one Member State from accessing data (stored by service providers) belonging to public authorities in other Member States by means of a European production order. If the authority is located in the issuing state, no restriction applies. The reasoning behind this is that the authorities of the issuing state can use their national instruments if the data is stored by a provider with addressees in the country. If, on the other hand, the authority has chosen a provider with addressees in another EU country, this is a coincidence from an investigative tactical point of view. Investigators should not be disadvantaged compared to a purely national constellation, which is why the instruments of Regulation (EU) 2023/1543 should be available to them. For cases in which a service provider stores or otherwise processes data protected by professional secrecy within the framework of an infrastructure, the Regulation also contains a separate provision with restrictive collection requirements concerning content and traffic data (Article 5(9) of the Regulation). As in the case of public authorities, this provision ensures that foreign investigative authorities do not, in principle, have direct access to data stored by service providers on persons bound by professional secrecy. Instead, the data must be requested by means of other legal assistance (usually via a European investigation order), so that the authorities involved from the German end can check whether there is a prohibition on seizure in accordance with §§ 97(1)(3) and 53(1)(3) StPO. An exception to this principle applies in the following cases: The individual concerned is a resident of the issuing state (but has stored their data with a service provider located in another Member State), Article 5(9)(a) of Regulation (EU) 2023/1543. The rationale for this provision is the same as that applicable to domestic authorities (see above). This means that only German investigative authorities, who must comply with the seizure prohibitions set out in the Code of Criminal Procedure, have, by means of a European production order, access to data (stored by service providers) relating to individuals subject to professional secrecy who are residents of Germany. Additional exceptions apply if an order addressed to the professional subject to professional secrecy could jeopardise the investigation (Article 5(9)(b) of the Regulation) and if professional secrecy has been lifted in accordance with the applicable law (Article 5(9)(c) of the Regulation). The law of the issuing state is decisive in determining whether the data is subject to professional secrecy.

In general, orders for the production of content or traffic data are subject to the notification requirement of Article 8 of the Regulation: The orders must be addressed in the form of a European production order certificate (EPOC) not only to the addressee of the service provider concerned (Article 9 in conjunction with Article 7 of the Regulation), but also to a designated authority in the executing state. The notification is only omitted if there are sufficient grounds to believe that both the place where the offence was committed and the place of residence of the person concerned by the data request are located in the issuing state (Article 8(2) of the Regulation). The notified authority shall examine the order on the basis of a list of grounds for refusal (fundamental rights, immunities and privileges, freedom of the press, ne bis in idem, double criminality; Article 12(1) of the Regulation). Except in urgent cases (Article 10(4) of the Regulation: eight hours), a period of ten days is provided for this purpose, during which the service provider may not produce the data (suspensive effect; Article 10(2) of the Regulation) and must first secure it (Article 10(1) of the Regulation). If the notified authority asserts a ground for refusal, the issuing authority must revoke the order; the service provider may not transmit the data (Article 12(2) of the Regulation). Otherwise, the service provider must hand it over to the issuing authority

after the expiry of the review period (ten days or earlier if the notified authority confirms that it does not intend to raise any grounds for refusal, Article 10(2) of the Regulation).

Orders for the production of subscriber and identification data, as well as preservation orders, are not subject to a notification requirement. The service provider must secure the data immediately (Article 10(1), Article 11(1) of the Regulation) and, in the case of production orders, transmit it within ten days at the latest (in emergencies immediately, within eight hours at the latest) (Article 10(3) and (4)(1) of the Regulation). If only preservation is ordered, this must be done for 60 days, extendable in principle by 30 days (Article 11(1) of the Regulation).

For cases in which a service provider does not comply with an order addressed to it, Article 16 of the Regulation provides for enforcement proceedings. Within this framework, the service provider has the option of raising objections to the execution of the production or preservation order based on a catalogue of reasons (Paragraph 3(a)). In addition to formal aspects such as lack of jurisdiction on the part of the issuing authority, these grounds also include immunities and privileges as well as freedom of the press (Paragraph 4(a) to (f), Paragraph 5(a) to (e)). The executing authority also examines the relevant catalogue, which is extended to include cases of obvious violations of fundamental rights (Paragraph 4(g), Paragraph 5(f)). If the service provider considers that complying with a production order would violate its legal obligations towards a third country, it may initiate the review procedure provided for in Article 17 of the Regulation. In the course of this procedure, a court in the issuing state may decide whether the order should be upheld. If the service provider violates the obligations imposed on it by Articles 10, 11 and 13(4) of the Regulation, the penalties provided for in Article 15 of the Regulation shall be imposed.

With regard to production orders, the Regulation provides for the right of persons affected by the data request to effective legal remedies in the issuing state. The fundamental rights guarantees in the executing state remain expressly unaffected, as do other legal remedies under national law (Article 18). The person whose data is requested must, in principle, be informed of the production without delay (Article 13(1) of the Regulation). In the interests of secure and rapid data exchange between authorities and addressees, Articles 19 et seq. of the Regulation provide for the creation of a decentralised IT system. Member States shall enable service providers to access this via their respective national IT systems, and service providers shall ensure that their addressees can use the system (Article 19(2) and (3) of the Regulation). The Regulation provides for standardised forms in the annexes for sending orders and for other communication purposes.

Pursuant to Article 14 of the Regulation, service providers may apply to the issuing state for reimbursement of their costs for providing information, in the case that this is provided for in comparable national situations. Reimbursement shall be carried out in accordance with the relevant national law. As the relevant regulations in Germany in Annex 3 to the Judicial Remuneration and Compensation Act do not contain any restrictions on German service providers, service providers from other Member States may also invoke them.

2. Directive (EU) 2023/1544

The accompanying directive requires that service providers establish one or more addressees within the EU so that decisions and orders to collect electronic evidence in criminal proceedings can be received and complied with.

This includes not only orders issued on the basis of Regulation (EU) 2023/1543, but also orders and decisions based on Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (Directive 2014/41/EU) and the Convention of 29 May 2000, drawn up by the Council, on Mutual Assistance in Criminal Matters between the Member States of the European Union, in accordance with Article 34

of the Treaty on European Union (Article 1(2)(1) of Directive (EU) 2023/1544). The mutual legal assistance procedures provided for in the two instruments remain unchanged (see below for details). Finally, Directive (EU) 2023/1544 applies to national orders and decisions to collect electronic evidence in criminal proceedings issued by an authority to addressees in its territory (Article 1(2)(2) of the Directive). Irrespective of this, direct data requests by national authorities to service providers established in their territory remain possible (Article 1(3) of the Directive). Direct data requests on one's own territory and on foreign territory in the context of security or for the purpose of fulfilling the central office function remain unaffected, as they are not covered by the scope of Directive (EU) 2023/1544.

According to Article 3 of the Directive, Member States must ensure that all service providers whose activities extend to the territory of the European Union establish a contact point there (Paragraph 1). This must be located in a Member State that applies the above-mentioned legal instruments and in which the services are actually offered (Article 3(2)(a) of the Directive). The Directive distinguishes between two types of addressees, namely 'designated establishments' and 'representatives', according to the following system: If service providers already have one or more establishments in an EU Member State that applies the above-mentioned legal instruments, they must designate one or more of them as addressees as defined by the Directive (Article 3(1)(a)). If establishments are located only outside the EU or in Member States that do not apply the aforementioned legal instruments, service providers must appoint one or more representatives (Article 3(1)(b) and (c)). Within the scope of the Directive, Member States may not impose obligations on service providers that go beyond their content, in particular with regard to the designation of notified establishments or the appointment of representatives (Article 1(4) of the Directive). This does not apply to the area of security or the exercise of a central office function, as these are not covered by Directive (EU) 2023/1544 (see above). Member States must designate one or more central authorities to ensure the consistent application of the Directive (Article 6(1) of the Directive). To this end, they must coordinate and cooperate with each other and, where appropriate, with the European Commission (Article 6(3) of the Directive). Member States must provide for penalties in the event that service providers fail to comply with their obligations in relation to the establishment of addressees (Article 5 of the Directive).

IV. Main content of the draft

The provisions of Directive (EU) 2023/1544 and the implementing provisions of Regulation (EU) 2023/1543 must be standardised in a newly created parent act. This creates a uniform legal framework and ensures that the e-evidence-specific regulations are practical and user-friendly.

In addition to a series of new regulations, the implementation of the Directive also requires adjustments to national law: In order to comply with the prohibition in Article 1(4) of Directive (EU) 2023/1544, which prohibits imposing obligations on service providers that go beyond the scope of the Directive, the applicability of national regulations requiring the appointment of authorised representatives in the context of the implementation of surveillance measures and information obligations for criminal proceedings, as provided for in the Telecommunications Act, must be restricted. The draft law also creates the necessary legal basis for data processing to fulfil the obligations under Regulation (EU) 2023/1543 with the amendments to the TDDDG.

The law is divided into four articles. Article 1 deals with the transposition of Directive (EU) 2023/1544 and the implementation of Regulation (EU) 2023/1543. Article 2 contains the necessary amendments to the Telecommunications Act, Article 3 contains the amendments to the Telecommunications Digital Services Data Protection Act. Article 4 provides for the Act's entry into force.

Article 1 is structured into four parts as follows: General regulations, transposition of Directive (EU) 2023/1544, implementation of Regulation (EU) 2023/1543 and provisions on fines and restriction of a fundamental right.

1. Part 1: General regulations

With regard to the definitions applicable to the Act, § 1 refers to the definitions in Article 3 of Regulation (EU) 2023/1543. It also specifies that the term 'addressee' is used as defined by Article 7(1) of Regulation (EU) 2023/1543.

2. Part 2: Transposition of Directive (EU) 2023/1544

In accordance with § 2, the provisions of Part II implementing Directive (EU) 2023/1544 apply not only to decisions and orders pursuant to Regulation (EU) 2023/1543, but also to those based on Directive 2014/41/EU and the Convention of 29 May 2000, drawn up by the Council, on Mutual Assistance in Criminal Matters between the Member States of the European Union, in accordance with Article 34 of the Treaty on European Union. They also apply to national orders in criminal proceedings issued by a German investigating authority to an addressee (as defined by § 3(1) to (3) of this Act) on German territory (see below for details).

The core of the provisions is the obligation of service providers in § 3 to designate establishments or appoint representatives. The addressees must report these to the Federal Office of Justice in accordance with § 4, stating their contact details and the official language to be used in communication, or, in the case of addressee institutions in other Member States of the European Union, to the central authorities there.

The duties of the Federal Office of Justice as the central authority are summarised in § 6. Among other things, it monitors compliance with the service provider obligations under §§ 3 and 4 and transmits the information received from the service providers to the European Judicial Network in criminal matters.

3. Part 3: Implementation of Regulation (EU) 2023/1544

Part 3 includes three chapters: General provisions, European Production Orders and legal protection.

Chapter 1 covers the general provisions. § 7 contains a general reference to the provisions of the Courts Constitution Act and its implementing act, as well as to the provisions of the Youth Courts Act and the Code of Criminal Procedure. The reference applies insofar as no specific procedural requirements arise from Part 3 of this Act and Regulation (EU) 2023/1543.

Chapter 2 contains the implementing provisions for European production orders. § 8 first links the differing terminology used in the Regulation and in national law. § 9 provides for the competence of courts and public prosecutors to issue and validate orders for the production of subscriber data and data requested solely for identification purposes in accordance with Article 4(1)(a) of Regulation (EU) 2023/1544. As other competent authorities as defined by Article 4(1)(b) of the Regulation, § 9(2) names a number of secondary competent authorities in accordance with national regulations on inventory data disclosure (investigators from the public prosecutor's office, tax authorities and customs authorities). § 9(3) and (4) provide for the procedure and responsibilities in the public prosecutor's validation procedure. § 10 addresses the authority to issue orders for the production of particularly sensitive traffic and content data pursuant to Article 4(2) of the Regulation, which lies with the courts. Paragraphs 2 and 3 relate to the procedure and the responsibilities in the remission procedure. § 11 designates the competent executing

authority. Finally, §12 provides for the statistical obligations of the judicial administrations of the Federal States and the Federal Prosecutor General.

Chapter 3 provides for legal protection.

Section 1 deals with appeals against outgoing orders. The provisions of the Code of Criminal Procedure, which are also applicable in the case of national orders, are applicable, to which reference is made in § 13 – subdivided according to the various data categories – shall apply to these orders. In accordance with § 14(1), the court seised shall substantively examine whether the provisions of Articles 4 and 5 of Regulation (EU) 2023/1543 have been complied with.

Section 2 deals with the procedure in the event of conflicting obligations under Article 17(3)(2) of the Regulation. Pursuant to §15, the Higher Regional Court or, in the case of preliminary investigations by the Federal Prosecutor General, the Federal Court of Justice is responsible for the decision to be made here. The decision shall be made by way of an order which cannot be appealed (§16).

Section 3 concerns appeals against decisions in enforcement proceedings and declares the provisions of the Administrative Offences Act to be applicable.

4. Part 4: Provisions on fines and restriction of a fundamental right

The fourth part of the Act lays down in § 18(1) the provisions on fines transposing Article 5(1) of Directive (EU) 2023/1544 and § 18(2) those implementing Article 15(1) in conjunction with Article 16(10) of Regulation (EU) 2023/1543. § 18(1) is ancillary to the set-up, notification, equipment and cooperation obligations of the service providers. § 18(2) is ancillary to the obligations of service providers to set up, notify, equip and cooperate.

§ 19 (restriction of a fundamental right) takes into account the requirement to cite the law in accordance with Article 19(1)(2) of the Basic Law.

V. Executive footprint

No stakeholder representatives or commissioned third parties contributed significantly to the content of the draft.

VI. Alternatives

None. As the draft serves the mandatory implementation and enforcement of European legal acts, there are no alternatives.

VII. Legislative powers

The legislative power of the Federal Government for the provisions in Article 1 of the draft implementing Regulation (EU) 2023/1543 and transposing Directive (EU) 2023/1544 is derived from Article 74(1)(1) of the Basic Law (criminal law, judicial proceedings). The provisions in Articles 2 and 3 of the draft amendment to the Telecommunications Act and the Telecommunications Digital Services Data Protection Act are based on the legislative powers under Article 73(1)(7) of the Basic Law (telecommunications) and Article 74(1)(11) of the Basic Law in conjunction with Article 72(2) of the Basic Law. Federal legislation is necessary here in order to maintain legal uniformity in the interests of the state as a whole. A diversity of legislation at Federal State level would create unreasonable

obstacles to cross-border legal transactions would therefore run contrary to the objective of the Act to increase the efficiency of criminal prosecution in the Federal Republic of Germany and in the European Union. Insofar as service providers are requested to provide information in the area of mutual legal assistance by law executing authorities of other Member States, uniform standards must apply nationwide, regardless of the location of the addressee.

VIII. Compatibility with European Union law and international treaties

The draft serves to implement Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 and is compatible with European Union law. The draft is also compatible with the international treaties concluded by the Federal Republic of Germany. The obligations under 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 EU No L 241 p. 1 from 17.09.2015) have been observed.

IX. Impact of the legislation

1. Legal and administrative simplification

Regulation (EU) 2023/1543 is directly applicable law in the Federal Republic of Germany, but must be supplemented by implementing provisions in order to achieve the intended effect in the area of national legislation. The implementing provisions will be laid down together with the provisions for transposing the directive in a new parent act so that all relevant national provisions can be found in one place in the clearest possible manner for those applying the law. The provisions of the draft help to avoid legal uncertainties in the area of European preservation and production orders, thereby leading to a clearer legal situation.

2. Sustainability aspects

The draft is in line with the guiding principles of the German Federal Government on sustainable development as set out in the German Sustainable Development Strategy (DNS), which serves to implement the United Nations resolution 'Transforming our world: the 2030 Agenda for Sustainable Development'.

By introducing European regulations for the collection of electronic evidence in criminal proceedings into the German legal system, the draft contributes to the achievement of sustainability 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'. In its target defined in 16.a, this sustainability goal calls for supporting the relevant national institutions, in particular through international cooperation in capacity building at all levels, to prevent violence and combat terrorism and crime. The draft promotes the achievement of this target by regulating the direct retrieval of electronic evidence by law executing authorities from electronic communications service providers in another Member State. The draft therefore strengthens cross-border cooperation in criminal matters between the Member States of the European Union. This will improve both national and Europe-wide efforts to combat crime and enhance security in the Federal Republic of Germany and in Europe.

By regulating the provision of administrative assistance by the Federal Office of Justice to the competent authorities of other Member States, including the transmission of information on the addressees of telecommunications service providers, the draft also

contributes to the achievement of target 16.6, which calls for the establishment of efficient, accountable and transparent institutions at all levels.

The draft thus follows the sustainability principles of the German Sustainability Strategy '(1.) Consistently apply sustainable development as a guiding principle in all areas and in all decisions' and '(5.) Preserve and enhance social cohesion in an open society'.

3. Budget expenditure excluding compliance costs

The Act will result in additional expenditure for the Federal Government.

With the entry into force of the Act in 2026, based on the case numbers set out in 4.2.1 for the specialised tasks, it is currently estimated that there will be one-off staffing requirements for a period of one year totalling 4.0 FTEs at the senior civil service level (consisting of 1.3 FTEs A15 and 2.7 FTEs A14), 4.6 FTEs at the upper civil service level (A12) and 3.8 FTEs at the middle civil service level (A9m). This will result in estimated one-off personnel costs of EUR 1 216 000. Personnel requirements are higher in this case due to the initial setup of the addressees by the service providers subject to the obligation, which will result in a high volume of cases to be processed.

From 2027 onwards, there will be a permanent, annual staffing requirement for specialised tasks and IT tasks totalling an estimated 1.9 FTEs at the senior civil service level (consisting of 1.1 FTE A14 and 0.8 FTE A15), 3.7 FTEs at the upper civil service level (A12) and 2.0 FTEs at the middle civil service level (A9m). Overall, the permanent staffing requirement is estimated at EUR 741 000 per year. The Federal Office of Justice (BfJ) will not require any additional staff to fulfil its statistical obligations, as this will only involve a few minutes of work per year.

The additional material and staffing requirements will be compensated for in individual plan 07 in terms of funds and jobs.

The Federal States will incur additional personnel costs estimated at EUR 273 000 in connection with their obligations in the administrative fine proceedings. No additional personnel costs are expected for the Federal States or for the Federal Prosecutor General in connection with the implementation of their statistical obligations. The additional expenditure is only estimated to be a few minutes.

4. Compliance costs

Compliance costs for businesses

Seq. No.	Article Draft regulation; standard (§§); designation of the requirement	IP	Annual number of cases and unit	Annual expenditure per case (minutes * labour costs per hour (business sector) + material costs in EUR)	Annual compliance costs (in thousands of EUR) or 'minor' (justification)	One-time number of cases and unit	One-off expenditure per case (minutes * labour costs per hour (business sector) + material costs in EUR)	Non-recurrent compliance costs (in thousands of EUR) or 'minor' (justification)
4.2.1	Article 1 EBewMG; § 3(1) to (3) and § 4; Obligations of service providers	Yes	900 service providers	EUR 136.4 = (155 / 60 * 52.80 EUR/hour (Sector: J))	123	9 000 service providers	EUR 136.4 = (155 / 60 * 52.80 EUR/hour (Sector: J))	1 228

Seq. No.	Article Draft regulation; standard (§§); designation of the requirement	IP	Annual number of cases and unit	Annual expenditure per case (minutes * labour costs per hour (business sector) + material costs in EUR)	Annual compliance costs (in thousands of EUR) or 'minor' (justification)	One-time number of cases and unit	One-off expenditure per case (minutes * labour costs per hour (business sector) + material costs in EUR)	Non-recurrent compliance costs (in thousands of EUR) or 'minor' (justification)
4.2.2	Article 1 EBewMG; § 3(4); obligations of service providers		1 service provider	EUR 2 886.40 = (3 280 / 60 * 52.80 EUR/h (Sector: J))	3	10 service providers	EUR 2 886.40 = (3,280 / 60 * 52.80 EUR/h (Sector: J))	29
Total (in thousands of EUR)					126-			1 256
of which information duties (IP)					123-			

Compliance costs for the authorities

Seq. No.	Article Draft regulation; standard (§§); designation of the requirement	Federal Government / State	Annual number of cases and unit	Annual expenditure per case (minutes * labour costs per hour according to hierarchy level + material costs in EUR)	Annual compliance costs (in thousands of EUR) or 'minor' (justification)	One-time number of cases and unit	One-off expenditure per case (minutes * labour costs per hour according to hierarchy level + material costs in EUR)	Non-recurrent compliance costs (in thousands of EUR) or 'minor' (justification)
4.3.1	Article 1 EBewMG; § 6(1); Tasks of the BfJ as supervisory authority	Federal Government	1 BfJ	EUR 559 547 = (188 153 / 60 * 67.60 EUR/h) + (361 292/ 60 *40.40 EUR/h) + (185 132/ 60 *33.80 EUR/h) + 0 EUR/h)	559	1 BfJ	EUR 947 550 = (393 842/ 60 * 67.60 EUR/h) + (450 849 / 60 * 40.40 EUR/h) + (355 474 60 * 33.80 EUR/h) + 0 EUR)	948
4.3.2	Article 1 EBewMG; § 12(1); Statistical obligations of judicial administrations of the Federal States	Federal State	16 judicial administrations of the Federal States		'minor' (minor effort per case)	0 judicial administrations of the Federal States	EUR 0 = (EUR 0 0)	0.0
4.3.3	Article 1 EBewG; § 12(1); Statistical obligations of public prosecutor's offices	Federal State	140 public prosecutor's offices		'minor' (minor effort per case)			
4.3.4	Article 1	Federal	1		'minor' (low			

Seq. No.	Article Draft regulation; standard (§§); designation of the requirement	Federal Government / State	Annual number of cases and unit	Annual expenditure per case (minutes * labour costs per hour according to hierarchy level + material costs in EUR)	Annual compliance costs (in thousands of EUR) or 'minor' (justification)	One-time number of cases and unit	One-off expenditure per case (minutes * labour costs per hour according to hierarchy level + material costs in EUR)	Non-recurrent compliance costs (in thousands of EUR) or 'minor' (justification)
	EBewG; § 12(1); Statistical obligation of the Federal Prosecutor General	Government	Federal Prosecutor or General		number of cases and minor expenditure per case)			
4.3.5	Article 1 EBewMG; § 18(1); Tasks of public prosecutor's offices for administrative fine proceedings	Federal State	140 public prosecutor's offices	EUR 1 839.00 = (396 / 60 * 43.90 EUR/hour (100% full-time equivalent) + EUR 1 550)	257			0.0
Total (in thousands of EUR)					816-			851-
of which at federal level					559-			851-
of which at state level (including municipalities)					257-			0-

4.1 Compliance costs for citizens

Citizens will not incur any compliance costs.

4.2 Compliance costs for businesses

Below is a description of the compliance cost estimate for businesses for each specification.

4.2.1 Obligations of service providers pursuant to § 3(1) to (3) and § 4

One-off compliance costs:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
9 000	155	52.80		1 228	
Compliance costs (in thousands of EUR)				1 228	

Change in annual compliance costs:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
900	155	52.80		123	
Change in compliance costs (in thousands of EUR)				123	

Compliance costs as defined by the provisions on the designation or appointment of addressees pursuant to § 3(1) to (3) and the notification obligations under § 4 shall be incurred if

- i. a service provider with an establishment exclusively or also in the territory of the Federal Republic of Germany, designates its establishment in Germany; or
- ii. the service provider is from another EU Member State, offers its services in Germany (among other places) and appoints its representative there;
- iii. if the service provider is based outside the EU, offers its services in Germany (among other places) and appoints its representative there.

For the purposes of further calculation, it is assumed that it is most cost-effective for service providers, regardless of their headquarters, to designate only one addressee, even if their services are offered in several countries. Since it can also be assumed that the addressee will likely be designated where the headquarters are located and that foreign service providers, especially those from outside the EU, will prefer to designate their representative in English-speaking areas, it is assumed that the constellations described in ii) and iii) will hardly ever occur in practice.

With regard to determining the number of cases, the first step is to examine which economic operators are affected by the regulation. These are:

- Electronic communications services:
 - o publicly available electronic communications services that, regardless of the network technology and terminal equipment used, provide access to the internet and therefore connections to virtually all internet termination points (§ 1(1) in conjunction with Article 3(3)(a) of Regulation (EU) 2023/1543, Article 2(4)(a) of Directive (EU) 2018/1972 and Article 2(2)(2) of Regulation (EU) 2015/2120);
 - o interpersonal communications services (§ 1(1) in conjunction with Article 3(3)(a) of Regulation (EU) 2023/1543, Article 2(4)(b) of Directive (EU) 2018/1972);
 - o services consisting wholly or mainly in the transmission of signals, such as transmission services used for machine-to-machine communications and broadcasting (§ 1(1), in conjunction with Article 3(3)(a) of Regulation (EU) 2023/1543 and Article 2(4)(c) of Directive (EU) 2018/1972);
- internet domain name and IP numbering services, such as IP address allocation services and domain name registration services, and data protection and proxy services associated with domain names (§ 1(1) in conjunction with Article 3(3)(b) of Regulation (EU) 2023/1543);
- other information society services (§ 1(1) in conjunction with Article 3(3)(c) of Regulation (EU) 2023/1543 and Article 1(1)(b) of Directive (EU) 2015/1535):
 - o services provided at a distance, without the simultaneous physical presence of the contracting parties,

- o electronically supplied services that are sent at the point of origin and received at the point of destination by means of electronic equipment for the electronic processing (including digital compression) and storage of data, and which are entirely transmitted, conveyed and received by wire, radio, optical or other electromagnetic means,
- o services provided at the individual request of a recipient, which are provided by transmitting data at individual request.

There are no official or unofficial statistics available on the number of companies affected. Based on

- i. analyses of the Business Register (URS) and the Inward Foreign Affiliates Statistics (IFATS) for the economic classes 61.20 (wireless communications), 61.30 (satellite telecommunications), 61.90 (other telecommunications excluding wireline telecommunications), 63.11 (web portals) and 63.99 (other information service activities),
- ii. the estimate for the law implementing Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC and implementing Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services and amending other laws (see printed paper 676/23, page 60 et. seq.) and
- iii. discussions with the Federal Office of Justice,

the total number of cases affected is estimated at around 10 000, with around ten percent of these involving service providers controlled from abroad. Based on the assumptions made above, this ten percent has not been taken into account in the estimate.

For the fulfilment of obligations, approximately 9 000 service providers are therefore taken into account for the one-off compliance costs. An annual fluctuation of ten percent (900 service providers) is assumed for the annual change in compliance costs. This percentage is a rough estimate, as no relevant information could be found for this either.

The assumed time expenditure of 155 minutes is composed of various standard values from the Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands in Regelungsvorhaben der Bundesregierung [Guidelines for Determining and Presenting Compliance Costs in Regulatory Projects of the Federal Government]. 60 minutes for familiarisation with the information obligation, 60 minutes for internal meetings, 30 minutes for filling out forms, labelling and marking, and five minutes for data transmission and publication.

The average wage rate for the economic sector J Information and Communication, amounting to 52.80 EUR/hour, is used as the wage rate.

This changes the annual compliance costs by around 123 000 EUR and results in one-off compliance costs of around EUR 1.2 million.

4.2.2 Obligations of service providers pursuant to § 3(4)

One-off compliance costs:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
10	3 280	52.80		29	
Compliance costs (in thousands of EUR)				29	

Change in annual compliance costs:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
1	3 280	52.80		3	
Change in compliance costs (in thousands of EUR)				3	

Service providers established in the Federal Republic of Germany or offering services within the territory of the Federal Republic of Germany must provide their addressees with the powers and resources necessary to comply with the decisions and orders.

The monitoring obligation of the BfJ applies to all service providers who have established their addressees within the territory of the Federal Republic of Germany.

The wage rate is taken from 4.2.1. This changes the annual compliance costs by around EUR 3 000 and results in one-off compliance costs of around EUR 29 000.

4.3 Compliance costs for the authorities

Below is a description of the compliance cost estimate for government agencies for each specification.

4.3.1 Duties of the Federal Office of Justice (BfJ)

One-off compliance costs for the Federal Government:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
1	393 842	67.60	0	444	
1	450 849	40.40	0	304	
1	355 474	33.80	0	200	
Compliance costs (in thousands of EUR)				948	

Change in annual compliance costs of the Federal Government:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
1	188 153	67.60	0	212	
1	361 292	40.40	0	243	
1	185 132	33.80	0	104	
Change in compliance costs (in thousands of EUR)				559	

As the central authority pursuant to § 6(1), the Federal Office of Justice monitors service providers in the fulfilment of their obligations under §§ 3 and 4. To this end, the it cooperates and coordinates with the central authorities of other Member States and, where necessary, with the European Commission. In doing so, the Federal Office of Justice assists the central authorities of the other Member States by providing all appropriate information and mutual assistance (§ 6(2)). The Federal Office publishes and updates the information received on the publicly accessible website of the European Judicial Network in criminal matters and on its own website (§ 6(3)). In addition, in the event of a violation of the obligations under §§ 3 and 4, the Federal Office of Justice is responsible for prosecuting and punishing the administrative offence in accordance with § 18(8)(1). Furthermore, the Federal Office of Justice notifies the Commission annually of which service providers have failed to comply with their obligations, which enforcement measures have been taken against them and which sanctions have been imposed on them (§ 6(4)). The Federal Office of Justice also collects the data specified in Article 28(2) of Regulation (EU) 2023/1543 and transmits it to the Commission annually (§ 12(2)).

A total of 1 200 164 minutes is expected to be spent on this in 2026. The work involved includes IT configuration and administration, checking initial registrations, liaising with service providers and central authorities, checking notifications and objections, and deciding on objections. The respective activities will be carried out by employees in the middle service (355 474 minutes), higher service (450 849 minutes) and senior service (393 842 minutes).

Based on the respective time expenditures and the respective wage cost rates in accordance with Annex 9 of the Guide to Determining and Presenting Compliance Costs in Federal Government Regulatory Projects (EUR 33.80 per hour at the middle service, EUR 40.40 per hour at the upper civil service and EUR 67.60 per hour at the senior civil service level) results in a one-off compliance cost of around EUR 948 000.

The total annual time required is 689 577 minutes, which is attributable in particular to the processing of change notifications from service providers, the review of the list of service providers to be monitored, the administrative offence proceedings conducted and the statistical obligations. In addition, there are further ongoing expenses for IT configuration and administration tasks. The activities are again divided between the different hierarchical levels, with 188 153 minutes allocated to middle service, 316 292 minutes to upper service and 188 153 minutes to senior service. After taking into account the respective time expenditures and wage cost rates, the annual compliance costs therefore amount to around EUR 559 000.

4.3.2 Statistical obligation of judicial administrations of the Federal States pursuant to § 12(1)

Change in annual compliance costs of the Federal States:

The judicial administrations of the Federal States collect the specified data from the public prosecutors' offices within their jurisdiction and transmit it to the Federal Office of Justice by 31 March of the year following the reporting year. This involves a table containing approximately ten items of information. The effort involved is due to the checking and sending of the data. Due to the low effort per case, it is assumed that there will only be a minor change in the compliance effort.

4.3.3 Statistical obligation of the public prosecutor's offices pursuant to § 12(1)

The change in the annual compliance costs incurred by public prosecutors' offices as a result of the obligations under § 12(1) cannot be reported at this time, as the European Commission has not yet taken a binding decision on the automation of statistical data collection within the decentralised IT system in accordance with Article 19 of Regulation (EU) 2023/1543. However, due to the minimal effort required per case, it is assumed that the change in compliance costs will be negligible.

4.3.4 Statistical obligation of the Federal Prosecutor General pursuant to § 12(1)

The change in the annual compliance costs for the Federal Government due to the obligations under § 12(1) cannot be reported at this time, as the European Commission has not yet taken a binding decision on the automation of statistical data collection within the decentralised IT system in accordance with Article 19 of Regulation (EU) 2023/1543. However, due to the small number of cases and the minimal effort required per case, it is assumed that the change in compliance costs will be negligible.

4.3.5 Tasks of the public prosecutor's offices in administrative fine proceedings pursuant to § 18(2)

Change in annual compliance costs of the Federal States:

Number of cases	Time requirement per case (in minutes)	Hourly pay (in EUR)	Material costs per case (in EUR)	Personnel costs (in thousands of EUR)	Material costs (in thousands of EUR)
140	396	43.20	1 550	40	217
Change in compliance costs (in thousands of EUR)				257	

A failure to comply with orders by service providers may result in administrative fine proceedings. A total time expenditure of 55 510 minutes is assumed. It is assumed that this also includes the time required if the service providers take legal action against the fines. In Germany, there are approximately 116 public prosecutor's offices and 24 prosecutor general's offices. Each public prosecutor's office can therefore expect to spend 396 minutes per year on this task. The wage rate for upper civil servants in the Federal States is set at EUR 43.20 per hour (Guidelines, p. 69).

According to feedback from the Federal States, imposing the fine results in additional expenditure. An auditor is commissioned to determine the total turnover of a service provider. According to the guide, material costs are incurred through expenses for the use of external services. Based on interviews with auditors, a standard value of EUR 155 per hour is applied. It is assumed that 10 hours of work are required per case, i.e. a total of EUR 1 550 per case.

This changes the annual compliance costs for the Federal States by around EUR 257 000.

5. Other costs

For the purposes of these regulations, the effects of relief and burden on the issuing and validating authorities under §§ 9 and 10, as well as the burden on the competent public prosecutors' offices, local and higher regional courts due to the legal protection provisions in §§ 13 to 17, as well as the activities of the public prosecutors' offices as executing authorities pursuant to § 11(1) when receiving notifications in accordance with Article 8 of Regulation (EU) 2023/1443.

As national authorities will no longer need to be involved in all data requests from other EU countries in the future, this will result in a reduction in workload. With regard to the amount involved, the European Commission's cost estimate (see page 99 of the impact assessment; Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings) estimates a maximum of EUR -7.2 million for all Member States.

The Commission based its estimate of the cost changes on the number of annual requests to the five largest service providers. Germany ranked first with around 35 000 requests, accounting for around 38 percent of all requests from the EU (see impact assessment cited above, page 15). To calculate the additional costs of the two implementation projects, the figure of EUR -7.2 million must therefore be put into perspective and corresponds to around EUR -2.7 million (EUR -7.2 million * 0.38).

6. Other legal consequences

No effects relating to equality policy or consumer policy are to be expected. The same applies to demographic effects.

X. Time limit; evaluation

As the regulations implement European requirements and Directive (EU) 2023/1544 and Regulation (EU) 2023/1543 apply indefinitely, a time limit is not applicable.

No evaluation is required with regard to the administrative implementation of the European Union legal acts; an assessment will be carried out at European level in accordance with Article 33 of Regulation (EU) 2023/1543. Under Article 33 of Regulation (EU) 2023/1543, the European Commission is required to carry out the evaluation by 18 August 2029 at the latest and to submit an evaluation report to the European Parliament, the Council of the European Union, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights.

B. Specific part

Re Article 1 (Act on European Production Orders and Preservation Orders on Electronic Evidence)

Re Part 1 (General regulations)

Part 1 contains general, overarching provisions on both the implementation of Directive (EU) 2023/1544 and the enforcement of Regulation (EU) 2023/1543.

Re §1 (Definitions)

§1 refers to Article 2 of Directive (EU) 2023/1544 and Article 3 of Regulation (EU) 2023/1543 for the definition of the terms used in the Act. For the term 'addressee', which is not defined there, reference is made to the use of the term in Article 7(1) of Regulation (EU) 2023/1543.

Re Part 2 (Implementation of Directive (EU) 2023/1544)

Part 2 contains the provisions for the implementing the Directive.

Re §2 (Scope)

§ 2 establishes the scope of application, thus transposing Article 1(2) and (3) of Directive (EU) 2023/1544.

Re Paragraph 1

Directive (EU) 2023/1544 has no impact on the substantive validity of Directive 2014/41/EU and the Convention on Mutual Assistance in Criminal Matters between the EU Member States (EU Mutual Assistance Convention). Electronic evidence can still be obtained through the mutual legal assistance mechanisms provided for in both instruments. The procedures remain unchanged; orders must therefore be addressed to an authority in the requested country and cannot be served directly on service providers. However, the local jurisdiction of the requested authority is determined by the location of the addressees established in accordance with Directive (EU) 2023/1544: The authorities of the Member State in which the addressee is located are responsible for executing requests under Directive 2014/41/EU and the EU-RhÜbk. For example, if a French service provider establishes an addressee in Sweden based on Directive (EU) 2023/1544, a European investigation order would have to be sent to the competent authority in Sweden and no longer (as was the case before the addressee was appointed) to a French authority.

§ 2(1)(4) of this Act clarifies that the addressees to be established in accordance with Directive (EU) 2023/1544 are also responsible for receiving purely national orders and decisions that have no cross-border connection as defined by the e-evidence package (see Article 1(1) and Article 3(3) of Regulation (EU) 2023/1543). If addressees are located within the territory of the Federal Republic of Germany, German investigative authorities can therefore use them for investigations based on the Code of Criminal Procedure (StPO). The reasoning behind this is that, from the perspective of the investigating authorities, it is a matter of chance in which territory an addressee is located. If the service provider has chosen German territory, all other Member States can proceed in accordance with Regulation (EU) 2023/1543 and use the addressee. The German authorities should have the same right on the basis of national orders.

Re Paragraph 2

Paragraph 2 stipulates that German investigating authorities may continue to contact service providers established in Germany in order to collect electronic evidence in criminal proceedings. Therefore, if a service provider has an establishment in Germany and has established an addressee in another Member State – thereby falling within the scope of Regulation (EU) 2023/1543 – this does not preclude investigative measures limited to Germany in accordance with Union law and national law. The background to this is that the e-evidence package is intended to put Member States in a better position, i.e. to facilitate their investigative activities. Existing possibilities are therefore not restricted. Furthermore, investigative powers outside criminal proceedings (e.g. in security, personal protection and witness protection procedures) remain unaffected, as these do not fall within the scope of the e-Evidence Regulation. Inquiries in centralised procedures also remain unaffected.

Re § 3 (Designated establishments and representatives (addressees))

The provision implements Article 3 of Directive (EU) 2023/1544 and provides for the details of the obligation of service providers to set up addressees. In accordance with Article 1(5)(1) of the Directive, this applies to all service providers whose services cover the European Union. In accordance with Article 3(2)(a) of Directive (EU) 2023/1544, the addressee must be established in a Member State in which the services are actually provided.

The basis for the obligation to establish an addressee facility in § 3 is, in implementation of Article 3(1) of the Directive, (primarily) the existence of an establishment or (secondarily) the provision of services in Germany. A distinction is made in terms of terminology: If an existing establishment is eligible as an addressee, it must be designated as a 'designated establishment'; if this is not the case, a 'representative' must be appointed.

Pursuant to Article 1(5)(2) of the Directive, an exception to the obligation to establish addressees applies only to providers who are established in the territory of a single Member State and offer their services only there.

Against this background, §3 provides for three basic scenarios. Firstly, there is the scenario in which establishments exist in Germany and also in other Member States of the European Union that apply the legal instruments referred to in § 2(1) (Paragraph 1). In addition, a special scenario is considered in which one or more establishments exist solely in Germany and the services are offered not only in Germany or exclusively in other Member States (Paragraph 2; if there is an establishment only in Germany, the services are only offered there, the Directive does not apply in accordance with Article 1(5)(2), see above). Finally, in the case of Paragraph 3, the service provider either has no establishment in the EU or only has an establishment in a Member State that does not apply the legal instruments listed in § 2(1) of this Act.

§3 of this Act does not provide for a situation in which there is no establishment in Germany but in another Member State that applies the legal instruments listed in § 2(1). In this case, the obligations under Article 3(1) of Directive (EU) 2023/1544 do not apply to the Federal Republic of Germany: As explained above, the primary connecting factor for the obligations is the existence of an establishment in one of the participating Member States. Once such an establishment exists, the Member State concerned must ensure that the addressee is correctly identified. The mere provision of services in the Federal Republic of Germany does not in itself give rise to an obligation; according to Article 3(1) of Directive (EU) 2023/1544, this is only the case if there is no establishment in one of the Member States that apply the legal instruments listed in § 2(1).

The reference to Paragraphs 4 and 5 in Paragraphs 1 to 3 clarifies that service providers must ensure that both the establishments to be designated and the representatives to be appointed have the powers and resources to comply with the decisions and orders, and that their designation must take place within the specified time limit.

Re Paragraph 1

Paragraph 1 implements Article 3(1)(a) of Directive (EU) 2023/1544 and concerns the first of the above-mentioned variants. There are establishments both in Germany and in other Member States which apply the legal instruments referred to in § 2(1). In this scenario, at least one of these establishments must be designated as the addressee. A Member State in which the services are offered must be selected. This follows from Article 3(2)(a) of the Directive. In the (likely very rare) case that services are not offered in any country of establishment, there is a conflict between the requirement of Article 3(2)(a) of the Directive on the one hand and that of Article 3(1)(a) of the Directive on the other: On the one hand, the addressee should be established where the services are offered, but on the other hand, if there are establishments in the relevant Member States, one of these entities must be selected. In the special case examined here, the latter obligation takes precedence. This follows from a purposive interpretation of Directive (EU) 2023/1544: It aims to streamline and optimise the processes involved in cross-border data retrieval. To this end, it is important to be able to draw on the resources of an existing establishment that is well-established in its routines. The consideration that the addressee states should also be those in which the services are offered for reasons of proximity to the subject matter is secondary in comparison. If this obligation were given priority here, a (new) representative would have to be appointed, meaning that tried and tested procedures could not be used. This could lead to a reduction in efficiency, which would not be in line with the directive.

Re Paragraph 2

Paragraph 2 relates to the second of the above-mentioned scenarios. It also implements Article 3(1)(a) of Directive (EU) 2023/1544, taking into account the specific provision of Article 1(5)(2) of the Directive: If an establishment is located on German territory, Germany is obliged to ensure that an addressee is designated. However, if, as in the scenario described in Paragraph 2, there is no other establishment in the EU, the obligation only applies if the service provider's offer is not limited to Germany. This means that the service provider either operates on the market both domestically and in other Member States or only in other Member States. In both cases, the establishment located in Germany must be designated as responsible. If no services are offered in Germany, there is again a conflict between the requirement of Article 3(2)(a) of the Directive on the one hand and that of Article 3(1)(a) of the Directive on the other. This conflict must be resolved in favour of designating the existing establishment (see above, Paragraph 1).

Re Paragraph 3

In the third of the above variants, the service provider either has no establishment in the EU or only has an establishment in a Member State that does not apply the legal instruments listed in § 2(1) of this Act. These cases are dealt with in Article 3(1)(b) and (c) of the Directive. If the service provider's offer extends to the territory of the Federal Republic of Germany, then Germany must ensure that an addressee is established. The service provider must then appoint a representative here or in a Member State that applies the legal instruments listed in § 2(1) (and where it offers services).

Re Paragraph 4

According to Paragraph 4, service providers subject to the Directive must provide their addressees with the powers and resources necessary to comply with the decisions and orders falling within the scope of the Act (§ 2(1)). This obligation applies both to service providers who have established their addressees in the territory of the Federal Republic of Germany and to those who have established their addressees in one or more other Member States but offer their services there.

Re Paragraph 5

Paragraph 5 implements Article 3(6) of Directive (EU) 2023/1544 and specifies the date by which service providers subject to the Directive must have established at least one addressee as defined by Paragraphs 1 to 3. A period of six months applies in principle: If the services are already being offered at the time the Directive enters into force, this means 18 August 2026. If the services are only offered after the date of entry into force of Directive (EU) 2023/1544, the addressee must be established six months after commencement of the service.

Re Paragraph 6

Paragraph 6 stipulates that the addressees of the service providers obliged under the Directive who are established in the territory of the Federal Republic of Germany or offer their services there must cooperate with the competent authorities when receiving decisions and orders pursuant to § 2(1) in accordance with the legal provisions specified therein. This general obligation of cooperation on the part of the addressees is not explicitly provided for in Directive (EU) 2023/1544. However, it can be inferred from the responsibility of Member States to monitor the proper receipt of decisions and orders by addressees, Article 3(4)(2) of Directive (EU) 2023/1544.

Re §4 (notifications and languages)

§4 implements Article 4 of Directive 2023/1544, according to which service providers must provide the central authorities to be designated in each Member State (see 6) with the contact details of their addressees and information on the language regime. The Directive links this requirement to the existence of an addressee on the one hand and the provision of services in the territory of the Member State on the other. The specific contact details to be provided are specified in the software (Court Data Base) made available by the European Commission for the notification of service providers. The data entered in the software forms is automatically transmitted to the Federal Office of Justice. If the Federal Office of Justice validates the data, an access account is created for the service provider and the information is made available for publication on a special website of the European Judicial Network in criminal matters. If the service provider's registration application is rejected, the notification must be resubmitted, taking into account the reasons for rejection provided by the Federal Office of Justice. This method of transmission complies with the text form requirement.

Re Paragraph 1

Paragraph 1 concerns cases where service providers have established an addressee in Germany. They must provide the Federal Office of Justice with their contact details and any changes thereto in writing (Article 4(1) of Directive 2023/1544).

Re Paragraph 2

Paragraph 2 provides for the situation in which service providers have established their respective addressees in the territories of other Member States of the European Union and have an establishment in the Federal Republic of Germany (Point 1) or offer services in Germany (Point 2). In such cases, they must provide the central authorities designated by the respective Member State of the European Union (in which the addressee is established) with the contact details of the addressees and any changes thereto in writing (Article 4(1) of Directive 2023/1544).

Re Paragraph 3

Paragraph 3 concerns cases where service providers have designated several addressees, either in their own country or (where applicable) in another Member State. In this scenario, the notices referred to in Paragraphs 1 and 2 must also specify the exact geographical area of jurisdiction of the respective addressee (Article 4(3) of Directive 2023/1544).

Re Paragraph 4

Paragraph 4 supplements the notification requirements of Paragraphs 1 and 2 with a requirement relating to the language policy: The service provider must indicate which official language(s) of the European Union may be used in communication with the addressee(s). If the addressee is located in the territory of the Federal Republic of Germany, German must be one of these languages (Article 4(2) and (3) of Directive 2023/1544).

Re Paragraph 5

Paragraph 5 clarifies that the notifications pursuant to to in Paragraphs 1 to 3 must be submitted immediately after the expiry of the respective deadline for the designation or appointment of the addressee. If any changes are made, these must be notified immediately after they take place. Such a term of notice is not explicitly provided for in the Directive; it merely provides for time periods for the establishment of the addressees as such (in this Act, § 3(5)). However, since the notifications are essential for the functioning of the E-Evidence mechanism, the interpretation of the Directive gives rise to an obligation to transmit them without delay: If it were left to the service providers to arrange for notifications to be sent only after a considerable delay, the decisions and orders falling within the scope of application could not be delivered as intended in the meantime. This would contradict the basic idea of the E-Evidence Package (maximising the efficiency of criminal prosecution). The Act therefore also provides for a time limit for the transmission of notifications.

Re § 5 (Joint responsibility of service providers and addressees)

§5 implements Article 3(5) of Directive (EU) 2023/1544.

Re Paragraph 1

Paragraph (1)(1) refers to Article 3(5)(1) of Directive (EU) 2023/1544. The provision arranges the joint responsibility of addressees and service providers for violations of the obligations arising for one of them from the legal instruments referred to in § 2(1) of this Act (Regulation (EU) 2023/1543, Directive 2014/41/EU, Convention drawn up by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union). If the decisions and orders falling within the scope of application for securing or collecting electronic evidence are not properly implemented, a fine may be imposed on both the

addressee and the service provider. Paragraph 1(2) implementing Article 3(5)(2) of Directive (EU) 2023/1544, stipulates that the absence of appropriate internal procedures between addressees and service providers cannot serve as justification for a breach of duty.

Re Paragraph 2

Paragraph 2(2) stipulates, in accordance with Article 3(5)(3) of Directive (EU) 2023/1544, that joint liability under Paragraph 1(1) and (2) shall not apply if the act or omission giving rise to the breach of duty constitutes a criminal offence in Germany.

Re § 6 (Central authority)

In accordance with Article 6(1) of Directive EU 2023/1544, Member States shall designate one or more central authorities to ensure consistent application of the law. Accordingly, § 6 contains the following provisions:

Re Paragraph 1

It follows from Paragraph 1 that the Federal Office of Justice acts as the central authority and, in this role, monitors compliance with the obligations arising for service providers and their addressees from §§ 3 and 4 (Article 6(1) in conjunction with Articles 3 and 4 of Directive EU 2023/1544). In doing so, the Federal Office of Justice monitors that the addressees cooperate with the competent authorities in accordance with the applicable provisions when receiving decisions and orders pursuant to § 2(1) (Article 3(4)(2) of the Directive, § 3(6) of this Act). This refers to the cooperation obligations for the addressees arising from the legal instruments referred to in § 2(1). The Federal Office of Justice is not responsible for monitoring compliance with each individual order, as enforcement measures in specific cases are the responsibility of the public prosecutor's office as the competent authority. However, the Federal Office of Justice is to act in cases under § 3(6), where there is evidence of systematic non-compliance. To ensure that the Federal Office of Justice is made aware of such cases, the guidelines for international criminal proceedings (RiVAST) should provide for notification by the public prosecutor's offices.

In order to fulfil its monitoring obligations, the Federal Office of Justice must obtain an overview of the group of service providers obliged by Directive EU 2023/1544 who could be considered for designation as addressees in the Federal Republic of Germany or who would be subject to sanctions under § 18(1) in the event of failure to designate an addressee. To this end, the Federal Office of Justice may collect and process the necessary data, including personal data. This provision takes account of the double-door model. This requires not only a power of transmission (which is yet to be created) but also a power to retrieve and process the relevant data at the recipient's end.

Monitoring also covers the proper provision of powers and resources to the addressees in accordance with § 3(4) (Article 4(2)(2) of Directive EU 2023/1544). In order to implement its monitoring obligations, the Federal Office of Justice may request information and evidence from the addressee.

Re Paragraph 2

Paragraph 2 lists the parties with which the Federal Office of Justice must cooperate and coordinate, namely the central authorities of other Member States and, where necessary, the European Commission. The central authorities of other Member States must be supported with all appropriate information and administrative assistance (Article 6(3) of Directive EU 2023/1544).

Re Paragraph 3

This paragraph implements Article 4(4) of the Directive. According to this, the Member States of the European Union must ensure that the latest information necessary for the application of the Directive is always available on a special website of the European Judicial Network in criminal matters. This is intended to enable the issuing authorities to proceed quickly and in a targeted manner when gathering electronic evidence. Pursuant to Paragraph 3, the Federal Office of Justice must forward the information received in accordance with §4 and any related updates to the European Judicial Network in Criminal Matters for publication immediately upon receipt. According to Article 4(4)(3) of the Directive, the information may be 'disseminated in order to make it more easily accessible to the competent authorities'. Against this background, the Paragraph 3(2) provides that the Federal Office of Justice shall also publish the information provided by service providers on its own website.

Re Paragraph 4

This paragraph provides for the obligation of the Federal Office of Justice to inform the Commission annually on which service providers have failed to fulfil their obligations under §§ 3 and 4 of this Act, which enforcement measures have been taken against them and which sanctions have been imposed on them.

Re Part 3 (Implementation of Regulation (EU) 2023/1543)

Part 3 contains the provisions for the implementation of the Regulation.

Re Chapter 1 (General provisions)

Re §7 (Applicability of other procedural and jurisdictional provisions)

Pursuant to §7 the provisions of the Courts Constitution Act and its Introductory Act, the Code of Criminal Procedure and the Youth Courts Act (JGG) apply accordingly, unless specific or conflicting procedural provisions are provided for in Regulation (EU) 2023/1543 or in this Act. The reference is intended to close gaps, for example with regard to the precise regulation of judicial jurisdiction and the organisation of the courts. The applicability of special provisions of the JGG shall be ensured in cases where the person affected by the data query is a juvenile or young adult as defined by §1 JGG. In cases involving a juvenile, this ensures that the provisions on the participation of legal guardians and legal representatives (in particular §§ 67, 67a JGG) apply.

Re Chapter 2 (European production and preservation orders)

The first chapter contains the standards on European production orders, in particular regarding their issuance, review and transmission.

Re §8 (Data categories for outgoing orders)

The terms used in Regulation (EU) 2023/1543 for the individual categories of data (see Article 3(8) et seq. of the Regulation) do not always correspond to the terminology used in German law. In addition, references to data categories can be found in various national laws. Against this background, §8 aims to harmonise the terms used in the Regulation on the one hand and in German law on the other, thereby ensuring greater certainty of application in the area of outgoing European production and preservation orders. The provision is an interpretative aid and does not restrict the scope of Regulation (EU) 2023/1543. On the one hand, not all data categories can be exhaustively covered, and on the other hand, the provision does not make any statement regarding incoming European

production and preservation orders. These must be observed and implemented by the addressees in the Federal Republic of Germany, irrespective of the present regulation.

The category of content data, which has not been legally defined in German law either, is completely omitted. The explanations provided in Article 3(12) of Regulation (EU) 2023/1543 sufficiently cover the possible cases of application. Relevant in national law may be various grounds for authorisation (e.g. §§ 94, 98; 95, 95a; 99 StPO, in the case of selective collection also §100a StPO).

Re Paragraph 1

Paragraph 1 deals with subscriber data as defined by Article 3(9) of Regulation (EU) 2023/1543 and links it to the category of inventory data in national law. According to the national definition standards in § 3(6) of the Telecommunications Act (TKG) and § 2(2)(2) of the Telecommunications Digital Services Data Protection Act (TDDDG), this refers to data that is necessary for the establishment, content design, modification or termination of a contractual relationship between the telecommunications service or digital service and the end user. It therefore concerns the contractual framework conditions that exist independently of a communication process. This regularly includes the name, address and registration information (such as email address) of the user. In addition, the term 'inventory data' also covers customer data that providers specified in § 172 TKG are obliged to collect, even if this is not necessary for operational reasons. Examples include the end user's date of birth, the telephone number assigned by the provider and, if a terminal device has been provided, its device number (IMEI number). All of these categories can also be found in Section F(a) of the form in Annex I to Regulation (EU) 2023/1543.

Re Paragraph 2

The same purpose as Paragraph 1 is pursued by Paragraph 2 with regard to data requested solely for the purpose of identifying the user (Article 3(10) of Regulation (EU) 2023/1543). This data corresponds to the usage data described in § 2(2)(3)(a) of the TDDDG. This refers to personal data of a user of digital services, the processing of which is necessary to enable the use of these services and to charge for them. In national law, however, the term 'usage data' goes beyond the term 'data requested solely for the purpose of identifying the user' as used in the Regulation and also includes, in § 2(2)(3)(b) and (c) of the TDDDG, data that, according to the terminology of the Regulation, falls under the term 'traffic data'. This is because Regulation (EU) 2023/1543 – unlike national law – does not distinguish between telecommunications services and digital services. Against this background, the reference in Paragraph 2 of the Act is limited to § 2(2)(3)(a) of the TDDDG and therefore to data that allows identification. This usually involves the last login IP address, including timestamp and port number, which can be used to identify the connection owner by means of a qualified inventory data query (see also the examples listed in Section F(b) of the form in Annex I to Regulation (EU) 2023/1543).

Re Paragraph 3

Finally, Paragraph 3 deals with traffic data as defined by Article 3(11) of Regulation (EU) 2023/1543 and refers to the national definition standard in the TKG (§ 3(70)). This refers to data that is necessary for the provision or billing of a telecommunications service, i.e. typically 'classic' connection data and, in the case of mobile connections, location data. It also includes other data falling under the national concept of usage data in § 2(2)(3)(b) and (c) of the TDDDG that goes beyond mere identification data (see above regarding Paragraph 2). This includes information about the digital services used and about usage. The data will regularly include information on the IP addresses, port numbers and data volume used.

Re §9 (Procedure for European production orders on subscriber data and identification data)

The provision is to be read in conjunction with §10. The two standards specify Article 4(1) and (2) of Regulation (EU) 2023/1543. This provides for which types of authorities the Member States can declare competent to issue European production orders. The Regulation follows a tiered approach based on the underlying understanding of the severity of the measures in question: According to this approach, production orders relating to content and traffic data that do not serve exclusively to identify the user are considered particularly intrusive. A production order is classified as less serious if it relates to subscriber and traffic data that serve exclusively to identify the user. Against this background, Article 4(1) and (2) of Regulation (EU) 2023/1543 each specify the type of authorities to which the final decision on the issuance of a production order may be assigned by the Member States of the European Union. In the case of more intrusive measures, this competence must be placed in the hands of a judge or court (Article 4(2) (a)), while in other cases this power may also be vested in a public prosecutor (Article 4(1) (a) of the Regulation). On the other hand, the Regulation opens up the possibility of designating authorities that are authorised to issue orders but that must have them validated by the primarily responsible authorities before sending them (Article 4(1) and (2), letter b in each case). Only in the emergency situation referred to in Article 4(5) – which is limited to subscriber and identification data – does the Regulation provide for an exception to the requirement of prior validation; this must be carried out within 48 hours.

The Regulation therefore specifies (in Article 4(1) and (2), letter a) a number of authorities to which the power to issue orders may be delegated. At the same time, however, it refers to the requirements of national law: Orders may only be issued if they could also have been issued in a similar form in a comparable national case under the same conditions (Article 5(2)(2) of the Regulation for the production order).

Against this background, §9 of the Act provides for the material and local jurisdiction of the respective issuing authorities as well as the validation procedure concerning subscriber data and identification data.

Re Paragraph 1

Paragraph 1 stipulates that the primary jurisdiction of the courts and public prosecutors for issuing European production orders to obtain subscriber data or data requested solely for the purpose of identifying the user in accordance with Article 4(1)(a) of Regulation (EU) 2023/1543 (and for the transmission of the corresponding certificate) is governed by Section 8 of Book I of the Code of Criminal Procedure. This contains the legal basis for data collection.

The following applies: The provisions on inventory data disclosure in § 100j(1)(1)(2) and (5) StPO do not contain any restrictive jurisdiction provisions, which is why public prosecutors' offices are also responsible for requests for information on inventory data in addition to the courts.

For the collection of data solely for the purpose of identifying the user, § 100k (3) StPO establishes the jurisdiction of the public prosecutor's office if the content of the use of the digital service is already known. However, if identification data is to be collected from digital services without the requirements of § 100k (3) StPO being met, or if the identification data is to be collected from telecommunications services, the courts have jurisdiction without exception (§ 100k (1) and (2), § 100g (1) and (2) StPO). In these scenarios, the procedure is governed by the provisions of § 10 applicable to traffic data, as explicitly referred to in Paragraph 5 (see below for details).

Since Article 9(1) of the Regulation distinguishes between the European production order and the associated certificate (European production order certificate = EPOC, see above) and the relevant competences in the validation procedure differ (see Paragraph 3), this Act takes both points of reference into account.

Re Paragraph 2

Paragraph 2 is based on Article 4(1)(b) of Regulation (EU) 2023/1543. This authorises Member States to designate additional competent authorities that may issue European production orders for subscriber data and data requested solely for the purpose of identifying the user, but which must be validated by a judge, court, investigating judge or public prosecutor (see above). Paragraph 2 confers secondary issuing powers on the authorities listed therein, insofar as they are authorised to take criminal proceedings under national law. This addition ensures that the designated authorities are not granted any further powers in implementing the Regulation than they would have in a purely national context. No new powers are therefore created for the respective authorities. The restriction to 'law enforcement' also clarifies that more extensive national powers to collect data – such as for the purpose of averting danger – are not covered by the provisions.

Point 1 lists the investigators of the public prosecutor's office who may also request inventory data information in national cases pursuant to § 100j(1)(1) StPO. 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 merely secondary competent issuing authorities, whose orders require validation by the public prosecutor's office, results from the wording of the Regulation (which refers to the 'public prosecutor's office' in Article 4(1)(a)) and the case law of the European Court of Justice on the European Investigation Order, which deals with a comparable question of interpretation (judgment of 2 March 2023, Case C-16/22).

Re Paragraph 3

Paragraph 3 provides for the validation procedures for the cases referred to in Article 4(1)(b) of Regulation (EU) 2023/1543. The Regulation does not standardise the procedure; this Act contains the necessary provisions. Where an issuing authority may act pursuant to Paragraph 2, it shall transmit its order to the public prosecutor's office in accordance with the Paragraph 3(1). 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 shall verify the legality of the order on the basis of the conditions set out in Regulation (EU) 2023/1543 (see below § 14(1) of this Act). In the event of validation, the public prosecutor's office shall transmit the order in the form of a certificate (EPOC) to the addressee. This is also done using the decentralised IT system and the reference implementation software provided by the Commission (Article 22 of the Regulation), which provide the necessary procedures and information for forwarding the order. The public prosecutor's decision on validation and, where applicable, the transmission of the EPOC to the addressee must be recorded in the file.

Re Paragraph 4

Paragraph 4 provides for local jurisdiction for validation (substantive jurisdiction is determined by Paragraph 3). According to Sentence 1, 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 standardises a procedure that deviates from Paragraphs 3 and 4 and refers to the procedures provided for in § 10(2) and (3). This provision is necessary because national law imposes different requirements for the collection of identification data. In the case of digital services, simplified collection of identification data by the public prosecutor's office is possible under the conditions set out in § 100k(3) StPO. If these conditions (knowledge of the content of the use) are not met or if data is to be collected from a telecommunications service, only judicial jurisdiction remains in accordance with § 100k (1) and (2) StPO or § 100g StPO (see above regarding § 8). In such cases, the procedure therefore corresponds to that of the order to produce traffic data, which is why reference is made to the procedures provided for in § 10(2) and (3).

Re §10 (Procedure for European production orders concerning traffic and content data)

Re Paragraph 1

Paragraph 1 refers to orders to produce traffic data, with the exception of data requested solely for the purpose of identifying the user and content data. The provision serves to implement Article 4(2)(a) of Regulation (EU) 2023/1543, according to which (only) a judge, a court or an investigating judge with jurisdiction in the case concerned may be granted the power to issue an order.

Under national law, according to Section 8 of Book I of the Code of Criminal Procedure, the courts are responsible for collecting traffic and content data, as the relevant legal bases for authorisation provide for a judicial review and urgent orders are excluded in these cases due to the structure of the Regulation (see Article 4(5) of the Regulation, which states that no ex post validation is permitted for traffic and content data).

Re Paragraph 2

Paragraph 2 contains more detailed provisions on the substantive and local jurisdiction of the courts. In order to embed the provisions of the Regulation in the national system of criminal prosecution, it is stipulated that the court's production order in preliminary proceedings must first be requested by the investigating authority under national law (public prosecutor's office, tax authority or customs administration authority). Sentence 2 declares that § 162(1)(1) and (3) and § 169 StPO shall apply accordingly. § 162(1)(1) concerns the appointment of the investigating judge in preliminary proceedings. The reference to § 162(3) StPO ensures that, after the public prosecution has been instituted, the court dealing with the case is responsible for issuing the production order. § 169 StPO is applicable accordingly in order to include the investigating judges of the Higher

Regional Court and the Federal Court of Justice in the scope of application. The reference to the provisions of the Fiscal Code and the Act to Combat Undeclared Work and Unlawful Employment is intended to cover situations in which the right to apply is assigned to authorities other than the public prosecutor's office. These are cases in which the customs and tax authorities conduct their own investigations and therefore submit applications to the courts with jurisdiction over them.

Pursuant to § 9(5), these provisions also apply to the collection of identification data, provided that this is the responsibility of a judge under national law.

Re Paragraph 3

Paragraph 3 provides for the remission procedure. The competent court shall examine whether the European production order can be issued on the basis of the conditions set out in Regulation (EU) 2023/1543. If this is the case, the court shall issue the order and transmit the corresponding certificate (EPOC) to the addressee using the decentralised IT system (Article 19(1) of the Regulation) and the reference implementation software provided by the Commission (Article 22 of the Regulation), which contain the necessary procedures and information for forwarding the order (see above). If the issuance of the production order is preceded by an application from the public prosecutor's office conducting the proceedings (or one of the other authorities referred to in Paragraph 2(1), the issuing authority may, if the application is rejected, lodge an appeal in accordance with §§ 304 and 306 StPO, as is the case with national powers. The last sentence of the paragraph concerns the documentation duty in the file for cases of both remission and rejection.

Pursuant to § 9(5), these provisions also apply to the collection of identification data, provided that this is the responsibility of a judge under national law.

Re §11 (Competent executing authority)

The provision specifies who acts as the executing authority pursuant to Article 3(17) of Regulation (EU) 2023/1543. The executing authority has two main tasks:

Firstly, it receives notifications in accordance with Article 8 of Regulation (EU) 2023/1543, which applies when content and traffic data (with the exception of data used exclusively for identification purposes) are requested. The corresponding production orders must not only be addressed to the designated establishment or representative of the service provider, but also to the executing authority (Article 8(1) of the Regulation), which must examine the information provided by the issuing authority to determine whether there are grounds for refusal (Article 12(1) and Article 8(3) of the Regulation). The RiVAST is to provide for a documentation duty for the executing authority regarding the result of the examination.

The duty to provide information only does not apply if there are sufficient grounds to believe that the place where the offence was committed is in the issuing state and that the person whose data is requested is resident in the issuing state (Article 8(2) of the Regulation). The Regulation describes the cases in which this can be assumed in Recitals 52 and 32. According to these recitals, the existing national provisions on jurisdiction in criminal proceedings remain unaffected. Therefore, § 7 of the German Code of Criminal Procedure (StPO) and § 9 of the German Criminal Code (StGB) must also be applied.

On the other hand, the executing authority is responsible for the procedure provided for in Article 16 of the Regulation for enforcement against service providers who do not comply with a preservation or production order. The executing authority must recognise and enforce the order transmitted to it by the issuing authority without further formalities (Article 16(1), (2) and (3)). In doing so, it formally requests the addressee of the service

provider to comply with its obligation and gives it the opportunity to comment (Article 16(3)). The addressee may then invoke the grounds for refusal set out in Paragraphs 4 and 5. If the authority ultimately determines that the order is enforceable and the addressee has not complied, a financial penalty shall be imposed in accordance with Article 15 of the Regulation.

Re Paragraph 1

Paragraph 1 designates the public prosecutor's office as the executing authority. The local authority with jurisdiction is the public prosecutor's office at the regional court in whose district the addressee of the order – that is, the named establishment or representative of the service provider – is located. The Federal States may adopt different rules for local jurisdiction, in particular to enable a concentration of jurisdiction in the sense of specialisation. This could be particularly useful in connection with the receipt of notifications, as the relevant infrastructure and expertise must be available here to process them within the shortest possible time.

Re Paragraph 2

Given the volatility of digital evidence, efficiency and speed are crucial in the procedures under Regulation (EU) 2023/1543. In some cases, it can be problematic if the issuing or requesting authorities of a Member State of the European Union are unclear about the competences in the requested Member State. If a domestic authority that is not competent receives a production or preservation order or a request (e.g. pursuant to Article 12(5)(1) of Regulation (EU) 2023/1543), it must forward it immediately to the competent authority and inform the issuing authority of the competent authority.

Re §12 (Statistical obligations)

Re Paragraph 1

Article 28(2) of Regulation (EU) 2023/1543 requires Member States to collect and maintain comprehensive statistical data and to submit it to the European Commission by 31 March each year. In order for the Federal Republic of Germany to comply with this requirement, the judicial administrations of the Federal States and the Federal Prosecutor General must first be obliged to collect the data from the competent authorities and transmit it to the Federal Office of Justice by 28 February of the year following the reporting year.

Article 28(3) of the Regulation stipulates that the data can be collected automatically, as the reference implementation software is programmed for this purpose. Separate data collection by the competent authorities is only necessary if the information is not generated through a direct chronological connection with the data transfer processes (e.g. appeals, missing ex-post validations and cost reimbursements, Article 28(2)(h) to (j)).

Re Paragraph 2

Paragraph 2 stipulates that the Federal Office of Justice shall compile an overview from the data obtained in accordance with Paragraph 1 and submit it to the European Commission by 31 March of the year following the reporting year at the latest.

Re Chapter 3 (Legal protection)

The second chapter provides for legal protection. The term is broadly understood and includes elements of the review process referred to in Article 17 of Regulation (EU) 2023/1543.

Re § 1 (Appeals against outgoing orders)

Re §13 (Applicable provisions)

The standard serves to implement Article 18 of Regulation (EU) 2023/1543. Under this provision, persons whose data has been requested by means of a European production order have the right to seek effective legal remedies against this order. §13 provides for the details in this regard.

Re Paragraph 1

Paragraph 1(1) refers to the provisions of the Code of Criminal Procedure that apply in comparable domestic cases for appeals against European production orders requesting subscriber data. In addition, Sentence 2 stipulates that the same appeals apply to data requested by the public prosecutor's office solely for the purpose of identifying the user. In practice, this concerns situations in which such identification data is collected by digital services. The decisive provision in this respect is § 100k(3) StPO, which allows the public prosecutor's office to retrieve identification data if it is already aware of the content of the use of the digital service. In the cases referred to in Sentences 1 and 2, the general legal remedies under § 98(2)(2) StPO (in the case of a public prosecutor's order or validation) or §§ 304(1), 306 and 310(2) StPO (in the case of a court order) are admissible.

If, following an appeal based on § 98(2)(2) StPO (against orders or validations issued by the public prosecutor), a judicial decision is issued, an appeal may also be lodged in accordance with § 304 StPO. However, the decision based on the appeal under § 304 StPO (against court orders) cannot be challenged by a further appeal under § 310 StPO. The provision is exceptional in nature and only applies to the serious measures specified therein. The orders in question here are significantly less intrusive, so that a corresponding application is not appropriate.

The provisions referred to in § 13(1) apply in the absence of specific regulations: National law does not contain an explicitly provided legal remedy for either § 100j StPO or § 100k(3) StPO. The provisions in §§ 100j(4) and 101a(7) StPO are limited to notification requirements without providing for any legal remedies.

Re Paragraph 2

Paragraph 2(1), on the other hand, refers to the more specific provisions in national law for traffic data as defined by the Regulation. As follows from § 8(3) of this Act, these include traffic data in accordance with the relevant provisions of the TKG and usage data in accordance with those of the TDDDG. Sentence 2 also stipulates that the same legal remedies apply to data requested by court order solely for the purpose of identifying the user. This applies, for example, to situations where identification data is collected for number-independent interpersonal telecommunications services. In national law, this measure – unlike the collection of data in the case of digital services, see above in Paragraph 1(2) – is subject to judicial review, §§ 100g(1), 101a(1)(1), 100e(1)(1) StPO.

In these cases, the provisions on data collection pursuant to § 100g(1) shall apply with regard to the collection of stored (retrograde) location data, also in conjunction with Paragraph 2, or § 100k(1) and (2) StPO, the time-limited legal remedies pursuant to § 101a(6)(2) in conjunction with § 101(7)(2) StPO. The relevant time limit begins with the notification of the data subject, which, according to Article 13(1) of the Regulation, must be made exclusively by the issuing authority. In the event that the data subject becomes aware of the data at an earlier point in time, the time limit begins at that point in time. Pursuant to § 101(7)(3), an immediate appeal may be lodged against the court decision in the case of both traffic and usage data.

Re Paragraph 3

Paragraph 3 provides for legal remedies against European production orders used to collect content data. In order to take into account all possible powers under national law, the reference includes the provisions of § 95a(5)(1) and (2) StPO (with regard to court orders for seizure pursuant to §§ 95 and 95a StPO), § 101(7)(2) and (3) StPO (with regard to judicial seizure pursuant to § 99 StPO and judicially ordered (selective) data collection pursuant to § 100a StPO) and §§ 304(1), 306, § 310 (2) StPO (with regard to the court order for seizure pursuant to §§ 94, 98 StPO).

In accordance with § 95a (5)(2) and § 101 (7)(3), an immediate appeal pursuant to § 311 StPO is admissible against the court decisions provided for therein; however, no further appeal against the decision pursuant to § 304 StPO is possible (see Paragraph 1). While the legal remedies pursuant to § 95a and § 101 (7) are subject to a time limit – again linked to the notification of the person concerned – no such time limit exists for the appeal option under § 304 StPO.

Re Paragraph 4

Paragraph 4 stipulates that the legal remedies provided for in Paragraphs 1 to 3 are only available to persons whose data has been requested. This clarification precludes service providers from taking legal action against the orders binding on them via the legal remedies provided for in §13. This is in line with the system of Article 18(1) of Regulation (EU) 2023/1543.

Re §14 (Judicial decision)

This provision provides for the standard of judicial review and the content and legal consequences of the decision on the appeal against production orders.

Re Paragraph 1

Paragraph 1 defines the scope of judicial review and refers to the conditions set out in Articles 4 and 5 of Regulation (EU) 2023/1543: While Article 4 of the Regulation provides for which authorities are competent to issue the orders (see above on §§ 9 and 10 of this Act), Article 5 contains the substantive conditions for issuing the orders. According to this, the production order must be necessary and proportionate and may only be issued if a similar order could have been issued in a comparable national case under the same conditions (Article 5(2) of the Regulation). The court must therefore apply a two-fold standard of review: Firstly, on the basis of Regulation (EU) 2023/1543, and secondly, on the basis of national law. The Regulation differentiates between the specific requirements depending on the type of data requested: If the data concerns subscriber data or data requested solely for the purpose of identifying the user, the production order may be issued for all offences (Article 5(3)). In other cases (other traffic and content data), one of the offences listed in Article 5(4)(b) of the Regulation must be involved, or the offence in the issuing state must be punishable by a maximum term of imprisonment of at least three years (Article 5(4)(a)). In both cases, the orders may also serve to enforce custodial sentences of at least four months or custodial measures imposed in criminal proceedings (provided that they have not been issued in absentia in cases where the convicted person has absconded). Article 5 of the Regulation also specifies the information that must be included in the production orders (Paragraph 5) and stipulates that they must, as a general rule, be addressed to the service provider acting as the controller as defined by Regulation (EU) 2016/679 (Paragraph 6). Article 5(8) and (9) of Regulation (EU) 2023/1543 contain specific requirements for cases where data is stored or otherwise processed within an infrastructure provided by service providers, public authorities or persons bound by professional secrecy (see III.1 above for more details).

Re Paragraph 2

Paragraph 2 provides for the legal consequences in cases where the conditions for issuing an order are not met. The court must determine the unlawfulness and revoke the European production order. With regard to data already obtained and the findings derived from it, it must be examined in each individual case, in accordance with the general principles of criminal procedure and data protection law, taking into account the seriousness of the procedural violation and the seriousness of the offence being prosecuted, whether the unlawfulness of the European production order gives rise to a requirement to delete data or a prohibition on use in criminal proceedings or use in criminal proceedings (see BVerfGE 130, 1; BGHSt 58, 32, 36, among others).

Re Section 2 (Procedure for conflicting obligations)

Re §15 (Judicial proceedings)

The standard provides for jurisdiction and procedure in the event of a request by the issuing authority pursuant to Article 17(3)(2) of Regulation (EU) 2023/1543. The provision applies if a service provider refuses to produce data on the grounds of conflicting legal provisions of a third country. If the issuing authority wishes to maintain its investigative measure despite the objection, it must apply for a court decision (Article 17(3)). The court examines the facts of the case and determines whether the order should be maintained. If the court concludes that there is no conflict of laws, the order remains in force (Article 17(5)). However, the court may also uphold the order despite the conflicting law of a third country if, after weighing up the circumstances, it concludes that the specific interests of the criminal investigation take precedence (Article 6 of the Regulation, which lists a number of factors to be given priority in the weighing up process).

Re Paragraph 1

According to Paragraph 1, legal recourse to the ordinary courts is available for applications for a decision on conflicts of law.

Re Paragraph 2

This paragraph determines the substantive and local jurisdiction: The High Regional Court in whose district the issuing authority has its seat shall decide on the application referred to in the Paragraph 1. The jurisdiction of the High Regional Courts is appropriate in view of the political significance of the decision to be taken (potential prioritisation of German criminal prosecution interests over the interests of the third country). Notwithstanding the jurisdiction of the Higher Regional Court pursuant to Sentence 1, the Federal Court of Justice shall have jurisdiction in cases where the order has been issued by the Federal Prosecutor General or the investigating judge of the Federal Court of Justice.

Re Paragraph 3

In accordance with Paragraph 3, the issuing authority shall attach to the request the outcome of its examination of the reasoned objection and any comments made by the executing state in accordance with Article 17(3)(1) of Regulation (EU) 2023/1543.

Re Paragraph 4

Pursuant to Article 17(2)(3) of Regulation (EU) 2023/1543, the reasoned objection must be raised no later than ten days after receipt of the production order by the addressee. § 15(4) refers to § 42 and § 43(2) StPO for the calculation of this period. The provision therefore also serves to implement Article 17(9) of the Regulation, according to which the time limits for the conflict proceedings are calculated in accordance with the national law of the issuing authority.

Re §16 (Judicial decision)

Article 17 of Regulation (EU) 2023/1543 provides for three possible decisions by the court: If it concludes that there is no conflict of laws, it shall uphold the production order (Article 17(5)). If, on the other hand, the court finds that there is a conflict, it may, after weighing up the relevant circumstances, either uphold or revoke the production order (Article 17(8)). §16 of this Act stipulates that the respective decision shall be made by way of an order from which no appeal lies.

Re Section 3 (Appeals against decisions in enforcement proceedings)

Re §17 (Applicability of the Administrative Offences Act)

§17 standardises the applicability of the Administrative Offences Act (OWiG) to legal remedies against decisions in enforcement proceedings in accordance with Article 16(10) of Regulation (EU) 2023/1543. The provisions in Section 5 OWiG apply to appeals against the fine notice, the subsequent court proceedings and the legal remedies.

Part 4 (Provisions on fines and restriction of a fundamental right)

Re §18 (Provisions on fines)

The provision serves to implement Article 5 of Directive (EU) 2023/1544 and to enforce Article 15(1) in conjunction with Article 16(10) of Regulation (EU) 2023/1543. It provides for offences subject to fines and the amounts of such fines. In all other respects, the provisions of the OWiG (§ 2 OWiG) apply. Both intentional and negligent infringements are sanctioned, as it follows from Recital 70 of the Regulation and Recital 19 of the Directive that all forms of infringement must be taken into account and the circumstances of the infringement must be taken into consideration.

Re Paragraph 1

Paragraph 1 contains the penalties for contravention of the obligations under §§ 3 and 4 of this Act.

Re Point 1

Paragraph 1(1) concerns the obligation of service providers to designate establishments, as stipulated in § 3(1) and (2). As the aforementioned Paragraphs of §3 also refer to Paragraphs 4 and 5, this covers cases in which the establishments are not designated in a timely manner or are not adequately equipped with powers and resources.

Re Point 2

§ 18(1)(2) concerns the obligation of service providers to appoint responsible representatives, as stipulated in § 3(3). As the aforementioned Paragraph of §3 also refers to Paragraphs 4 and 5, this covers cases where the representative is not appointed in a timely manner or is not adequately provided with powers and resources.

Re Point 3

Paragraph 1(3) refers to the obligation of service providers, as stipulated in § 4(1) and (2), to provide the competent central authority with the contact details of the addressees and to update these details where necessary. Due to the explicit reference to § 4(3) to (5), which can be found in both § 4(1) and (2), the other obligations mentioned there are also included: Accordingly, service providers must provide information on the language policy and, in the case of multiple designations, on the geographical scope of application, and must make the relevant notifications immediately after the expiry of the deadlines for the establishment of addressees specified in § 3(5) or immediately after changes occur.

Re Paragraph 2

Paragraph 2 contains the substantiation of the infringement of Articles 10, 11 and 13(4) of Regulation (EU) 2023/1543. The obligations laid down in Articles 10 and 11 primarily apply to the addressee as defined by §3 of this Act (see also Article 7 of the Regulation). In addition to the natural persons acting on behalf of the addressee, the applicability of §§ 30 and 130 OWiG also covers the responsibility of legal entities. In contrast, according to the wording of Article 13(4) of the Regulation, the obligation under that provision applies to both the addressee and the service provider.

Re Point 1

Paragraph 2(1) refers to the obligation of the addressee under Article 10(1) or (2)(2) of Regulation (EU) 2023/1543 to act upon receipt of an EPOC.

According to Article 10(1) of Regulation (EU) 2023/1543, the addressee must, immediately upon receipt of the production order, without delay and in a factual manner, secure all data covered by the request in such a way that subsequent production is possible.

Article 10(2)(2) of Regulation (EU) 2023/1543 provides for a special case relating to Article 10(2)(1) (see Point 2). In cases where the executing authority confirms within the ten-day period referred to in Sentence 1 that it will not invoke any grounds for refusal, the addressee must transfer the data as soon as possible, but no later than the expiry of the ten-day period referred to in Paragraph 1(1).

Re Point 2

Paragraph 2(2) reinforces the infringement of the addressee's obligation under Article 10(2)(1) of Regulation (EU) 2023/1543. This concerns the situation in which the issuing authority must notify the executing authority of the production order in accordance with Article 8 of Regulation (EU) 2023/1543. In this case, there is a period of ten days within which the executing authority may assert any grounds for refusal. If it fails to do so, the addressee must ensure that the data is transmitted immediately after the expiry of the time limit.

The issuing authority must notify the executing authority in accordance with Article 8(1) and (2) of Regulation (EU) 2023/1543 if it requests content data or traffic data that is not used exclusively for identification purposes; an exception applies in cases where both the person affected by the data query and the place of commission are located within the country.

Re Point 3

Paragraph 2(3) refers to the obligation of the addressee under Article 10(3) of Regulation (EU) 2023/1543. According to this, if no notification procedure is to be carried out, the data must be transmitted within ten days of receipt of an EPOC at the latest.

No notification is generally required under Article 8 of Regulation (EU) 2023/1543 for requests for subscriber data and traffic data used solely to identify the user. For content and other traffic data, see above.

Re Point 4

Paragraph 2(4), prohibits infringements of Article 10(4)(1) of Regulation (EU) 2023/1543. This stipulates the obligation of the addressee to transmit the requested data immediately in emergencies, at the latest within eight hours of receiving the EPOC.

The term 'emergency' is defined in Article 3(18) of Regulation (EU) 2023/1543 and describes a situation in which there is an immediate threat to the life, physical integrity or safety of a person, or in which the disruption or destruction of critical infrastructure may cause such a threat.

Re Point 5

Paragraph 2(5), prohibits breaches of the addressee's obligation to immediately inform the issuing authority and, in some cases, the executing authority that it is unable to comply with the production or preservation order for various reasons.

According to Article 10(6)(1)(1) of Regulation (EU) 2023/1543, this obligation applies if the addressee is unable to comply with its obligation to surrender because the EPOC is incomplete or manifestly incorrect or does not contain sufficient information. Article 10(7)(1) of Regulation (EU) 2023/1543 requires the addressee to inform the issuing authority if it is factually impossible for them to produce the requested data due to circumstances beyond their control. In cases where the production of data covered by EPOC is not possible for other reasons, Article 10(8)(1) stipulates the obligation of the addressee to inform the issuing authority thereof without delay.

All three provisions also require the addressee, in cases where the executing authority must also be notified of the production order in accordance with Article 8 of Regulation (EU) 2023/1543, to inform the executing authority of the above reasons in addition to the issuing authority.

Article 11(5)(1)(6)(1) and (7)(1) of Regulation (EU) 2023/1543 contain parallel obligations for the addressee of the preservation order to immediately inform the issuing authority of any incorrect or missing information in the EPOC-PR or other reasons that make it impossible to preserve the specified data.

The aim of these provisions is to ensure that obstacles to the processing and implementation of orders can be quickly identified and removed.

Re Point 6

Paragraph 2(6) stipulates that, in the event of a breach of the addressee's obligation under Article 10(6)(1)(2) of Regulation (EU) 2023/1543, the issuing authority must, at the same time as informing the addressee of an incorrect or incomplete EPOC, notify the addressee whether it was possible to identify and secure the requested data.

Re Point 7

The reinforcement in Paragraph 2(7) is based on the obligation of the addressee under Article 10(6)(2)(2) of Regulation (EU) 2023/1543 to ensure, in the event of notification of an incomplete or unclear EPOC, that it can also receive any clarification or correction of the EPOC by the issuing authority. The provision is intended to ensure an uninterrupted and rapid flow of information. A parallel obligation is laid down in Article 11(5)(2) of Regulation (EU) 2023/1543 for the receipt of a clarification or correction of an incomplete or incorrect EPOC-PR.

Re Point 8

Paragraph 2(8), concerns the obligation of the addressee to secure the requested data for the periods specified therein immediately upon receipt of an EPOC-PR in accordance with Article 11(1) of Regulation (EU) 2023/1543. In accordance with Article 11(1)(2) the retention period is generally 60 days from receipt of the EPOC-PR (unless the issuing authority confirms during this period that a request for production has been made; see also Point 10 below).

Re Point 9

Paragraph 2(9) concerns the obligation of the addressee to store the secured data for a further specified period after the expiry of the 60-day period. The prerequisite for this is that the issuing authority has requested this in accordance with Article 11(1)(3) during the 60-day period using the form in Annex VI and that the storage is necessary to enable a production order. The storage period is then a further 30 days.

Re Point 10

Paragraph 2(10) also concerns the obligation of the addressee under Article 11(2) of Regulation (EU) 2023/1543, which follows that of Article 11(1). It concerns scenarios in which data has been preserved on the basis of an EPOC-PR and the issuing authority confirms during the time periods specified in Article 11(1) of the Regulation that it has made a request for production. This may be a European production order, a European investigation order or another request for mutual legal assistance. In this situation, the addressee is obliged, in accordance with Article 11(2) of Regulation (EU) 2023/1543, to maintain the preservation of the requested data for as long as necessary to hand it over after receiving the request (or until the addressee has been notified that preservation is no longer necessary, Article 11(3) of the Regulation). The preservation period may therefore exceed the total period of 90 days specified in Article 11(1) of Regulation (EU) 2023/1543.

Re Point 11

Paragraph 2(11) refers to the obligation of the addressee and the service provider under Article 13(4) of Regulation (EU) 2023/1543 to adopt state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the certificates transmitted (EPOC or EPOC-PR) and of the data to be produced or secured.

Re Paragraph 3

Paragraph 3 determines the upper limit of a fine to be imposed and differentiates according to the nature of the infringement. In view of the principle of proportionality, a distinction is made between whether material core obligations of the regulations (with a high degree of unlawfulness) or other administrative and enforcement obligations (with a lower degree of unlawfulness) have been violated.

Re Point 1

Paragraph 3(1) stipulates that all cases referred to in Paragraph 1 and Paragraph (2)(1) to (4) and (7) to (11) may be punished with a fine of up to five hundred thousand euro.

The cases referred to in the Paragraph 1 initially refer to violations under § 3(1) to (3) and § 4(1) and (2) of this Act. These are merely administrative obligations relating to the establishment of the addressees and the communication of their contact details. However, these obligations are of central importance because they are the basic prerequisites for the functioning of the regulatory framework established by Regulation (EU) 2023/1543 and Directive (EU) 2023/1544. If the addressees do not exist or their contact details are unknown or incorrect, the orders cannot be transmitted as intended.

The cases referred to in Paragraph 2(1) to (4) and (7) to (11) concern violations of the fundamental obligations relating to the execution of European production orders and European preservation orders under Articles 10 and 11 of Regulation (EU) 2023/1543. This also includes ensuring accessibility for the issuing authority (Paragraph 2(7)), as functioning communication channels are a central element of Regulation (EU) 2023/1543, regardless of the specific context. Paragraph 2(11) sanctions violations of the equally fundamental obligation to ensure the confidentiality, secrecy and integrity of the EPOC in accordance with the current state of the art, as set out in Article 13(4) of Regulation (EU) 2023/1543.

The maximum fine is appropriate for the violation of these fundamental obligations. This is because seamless cooperation between service providers and their customers is essential in order to combat serious forms of crime, which are being facilitated by digital media on an unprecedented scale. A framework of sanctions is therefore necessary to act as an effective deterrent for service providers.

Re Point 2

According to Point 2, the cases referred to in Paragraph 2, Points (5) and (6) can be punished with a fine of up to one hundred thousand euro. The legal violations referred to here mostly concern the addressee's obligation to notify the issuing and executing authority in cases where data backup or production is impeded by various circumstances for which the provider is not responsible. These notifications are intended to enable the issuing authority to eliminate any problems that are predominantly within its sphere of influence and, if necessary, to adjust or withdraw the order. Against this background, the violations on the part of the service providers are to be classified as less serious. This is reflected in the lower maximum fine of one hundred thousand euro.

Re Paragraph 4

Paragraphs 4 to 6 implement the penalty provisions of Article 15(1)(3) of Regulation (EU) 2023/1543. The turnover-related fine contained therein is limited to the enforcement of obligations under Articles 10, 11 and 13(4) of the Regulation, as only these are expressly mentioned in Article 15(1)(1) of the Regulation as reference standards. In contrast, Article 5(2) of Directive (EU) 2023/1544 merely contains the usual general penalty clause ('Penalties must be effective, proportionate and deterrent') and therefore does not require a turnover-related financial penalty. This deliberate decision by the EU legislature is reflected here. The wording in Paragraph 4 is based on existing national regulations implementing sanction obligations under Union law.

Pursuant to Paragraph 4 in the case of a service provider with a total turnover exceeding EUR 25 million, by way of derogation from Paragraph 3(1)(b) a breach of an obligation under Paragraph 2(1) to (4) and (7) to (11) may be punished with a fine of up to 2 percent of that total turnover (and consequently with more than EUR 500 000). This provision ensures that even companies with strong financial resources face a significant fine for violating core obligations.

Re Paragraph 5

Paragraph 5 deals with less serious infringements under Paragraph 2(5) and (6). Contrary to Paragraph 3(2), these may be punished with a fine of up to 2 percent of total turnover (and consequently more than one hundred thousand euro) for service providers with a total turnover of more than EUR 5 million. The rationale behind this is the same as in Paragraph 4 (deterrent effect). Paragraph 5 also encompasses less serious infringements by service providers with a total turnover of more than EUR 25 million, as these companies automatically have a turnover of more than EUR 5 million.

Re Paragraph 6

Paragraph 6 specifies the methods for determining total turnover. The turnover for the financial year preceding the authority's decision shall be used as the basis. The service provider's annual turnover worldwide shall be included. The executing authority may estimate the total turnover.

Re Paragraph 7

Paragraph 7 stipulates that § 17(2) of the Administrative Offences Act does not apply to infringements under Paragraph 2. This prevents the maximum fine for negligent acts from being automatically reduced by law to half of the maximum penalty uniformly imposed for intent and negligence. Regulation (EU) 2023/1543 states in Recital 70 that all circumstances of the infringement must be taken into account, including whether the infringement was committed intentionally or negligently. Accordingly, the Regulation requires that negligent infringements also be punished. However, the penalty provision in Article 15(1)(3) of the Regulation does not distinguish between intentional and negligent infringements and therefore also applies to the latter. The Regulation does not provide for a regular reduction of the maximum amount of the threatened fine for negligent infringements, as provided for in § 17(2) OWiG. However, the manner in which the infringement was committed must be taken into account together with other circumstances when determining the amount of the fine, thereby also taking Recital 70 of Regulation (EU) 2023/1543 into account.

Re Paragraph 8

Paragraph 8 determines which authorities are administrative authorities as defined by § 36(1)(1) OWiG.

Re Point 1

Paragraph (8)(1) stipulates that the Federal Office of Justice is the competent administrative authority for administrative offences under Paragraph 1, which are linked to Directive (EU) 2023/1543. Pursuant to §6, it is also responsible for monitoring the obligations under §§ 3 and 4, for which Paragraph 1 provides for sanctions in the event of non-compliance.

Re Point 2

Point 2 specifies that the administrative authority for administrative offences referred to in Paragraph 2 is the executing authority pursuant to § 11(1). This authority is responsible for conducting enforcement proceedings in accordance with Article 16 of Regulation (EU) 2023/1543. Therefore, in accordance with Article 16(10) of the Regulation, it must also be the authority that imposes the penalties provided for.

Re §19 (Restriction of a fundamental right)

This provision complies with the citation requirement set out in Article 19(1)(2) of the Basic Law.

Re Article 2 (Amendment to the Telecommunications Act)

Articles 10, 11 and 19 et seq. of Regulation (EU) 2023/1543 and the implementing act to be adopted by the Commission pursuant to Article 25 of Regulation (EU) 2023/1543 contain numerous provisions on the technical implementation of production and preservation orders, the deadlines to be met, security standards and minimum availability targets. These apply directly and take precedence over the provisions of the Telecommunications Act (TKG).

However, there is a need for regulation with regard to the prohibition contained in Article 1(4) of Directive (EU) 2023/1544 on Member States imposing obligations on service providers that go beyond the obligations arising from the Directive. This prohibition relates in particular to the designation of notified establishments or the appointment of representatives. According to Recitals 1 to 3 of the Directive, this is intended to prevent Member States from imposing their own obligations on service providers to appoint addressees on their territory, as these could be incompatible with each other or conflict with Union law and could potentially be subject to different penalties. This would hinder the free movement of services in the internal market.

Against this background, national provisions on the appointment of representatives for service of documents must be declared inapplicable insofar as they fall within the scope of Directive (EU) 2023/1544, i.e. exclusively criminal proceedings. It should be noted that the material scope of the Directive is not limited to measures under Regulation (EU) 2023/1543: Rather, pursuant to Article 1(2) of Directive (EU) 2023/1544, it also covers the gathering of electronic evidence on the basis of Directive 2014/41/EU and the Convention pursuant to Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters. This means that the issuing State must also address requests under these instruments to the Member States in which the addressees designated under Directive (EU) 2023/1544 are located. However, unlike Regulation (EU) 2023/1543 (see Article 3(8) and Recital 19), the aforementioned legal instruments also allow the collection of real-time data, i.e. telecommunications surveillance in the context of criminal proceedings. In view of the prohibition contained in Article 1(4) of Directive (EU) 2023/1544 on imposing obligations that go beyond the scope of the Directive, national law may not require service providers to establish addressees in the area of telecommunications surveillance for law enforcement purposes. Therefore, the provisions contained in the Telecommunications Act must be declared inapplicable insofar as they require the appointment of authorised representatives for the purpose of implementing telecommunications surveillance for law enforcement purposes within the scope of Directive (EU) 2023/1544. This applies both to operators of telecommunications facilities used to provide publicly available telecommunications services (§ 170(1)(3)(b) TKG) and to providers of publicly available telecommunications services who use a telecommunications facility operator for this purpose (§ 170(2)(2)(c) TKG). This does not affect the obligations specified in § 170(1)(3)(b) TKG and § 170(2)(2)(c) TKG for the respective monitoring and interrogation powers outside of criminal proceedings (in

particular, hazard prevention and central office function). In this respect, the above-mentioned provisions and obligations remain valid within the framework laid down in § 1(2) of the Telecommunications Act.

Re Article 3 (Amendment to the Telecommunications Digital Services Data Protection Act)

Re Point 1

Point 1 contains the adjustments to the table of contents with regard to the insertion of Paragraphs 13a and 24a in the TDDDG.

Re Point 2

Point 2 contains the new § 13a. The regulation is necessary to enable providers of publicly available telecommunications services and their addressees to process personal data in order to comply with their obligations under Regulation (EU) 2023/1543. The addressees are the designated establishments and representatives that the service providers affected by the Regulation have established to fulfil their obligations under § 3(1) to (3) of the Act on European production and preservation orders for electronic evidence. Regulation (EU) 2023/1543 provides for the production or preservation of electronic evidence by service providers or their addressees in criminal proceedings on the basis of European production orders or European preservation orders issued by competent authorities in a Member State. These authorities may therefore require a service provider offering services in the Union and having designated an addressee in another Member State to receive orders to produce or preserve electronic evidence, regardless of where the data is located.

Regulation (EU) 2023/1543 does contain an obligation for addressees to comply with such production or preservation orders, but it does not contain any provision authorising the addressees or service providers to process personal data for this purpose. According to the case law of the Federal Constitutional Court, when establishing an information procedure based on its own powers, the legislature must create proportionate legal bases for both the transmission and retrieval of data (double door; BVerfG, decision of 27 May 2020 - 1 BvR 1873/13, 1 BvR 2618/13 -, para. 93).

In Germany, this requires a legal basis for data processing for the purpose of complying with this order (first door). Regulation (EU) 2023/1543 does not contain any corresponding provision. In addition, there must be a legal basis for the authority to request data (second door). In the case of European production and preservation orders from other EU Member States addressed to addressees in Germany, this legal basis can be found in Chapter II of Regulation (EU) 2023/1543 in conjunction with the national law of the respective other Member State.

Article 3(8) of Regulation (EU) 2023/1543 defines which data are considered electronic evidence. This data must be processed accordingly by or on behalf of a service provider upon receipt of a European production order certificate or a European preservation order certificate. Service providers, including electronic communications services as defined by Article 2(4) of Directive (EU) 2018/1972, are obliged to comply with a European production order or a European preservation order (Article 3(3)(a) of Regulation (EU) 2023/1543). These are generally internet access services provided for a fee, interpersonal communication services (both number-based and number-independent) and services consisting wholly or mainly in the transmission of signals, such as transmission services used for machine-to-machine communication and broadcasting. Purely business-related telecommunications services that are not offered commercially, i.e. without being part of

an economic consideration, such as the provision of telecommunications within companies or other organisations in the context of employment or service relationships, are not subject to production or preservation orders and therefore do not require authorisation for data processing.

Since traffic data are subject to telecommunications secrecy, which is infringed upon here, § 13a(2) complies with the citation requirement pursuant to Article 19(1)(2) of the Basic Law.

Re Point 3

As in Point 2, the digital services covered by Regulation (EU) 2023/1543 (or their addressees) also require a specific legal basis for the processing of personal data, without which a European production or preservation order addressed to these providers would be ineffective. Regulation (EU) 2023/1543 does not apply to all digital services (defined in the Regulation as information society services as defined by Article 1(1)(b) of Directive (EU) 2015/1535), but only to providers of digital services that enable their users to communicate with each other or to store or otherwise process data, provided that the storage of data is a defining feature of the service provided to the user. Accordingly, the necessary power to process data must also be limited to these providers. Digital services affected by European production or preservation orders include, for example, online marketplaces that enable consumers and businesses to communicate with each other, and other hosting services, including cloud computing services, as well as platforms for online games and online gambling. This does not include digital services that do not enable their users to communicate with each other, but only offer communication with the service provider. Digital services that do not enable their users to store or otherwise process data, or where data storage is not a determining, i.e. essential, part of the service provided to the user, such as in the case of online legal, architectural, engineering and accounting services, are also excluded (Recital 27 of Regulation (EU) 2023/1543). The Regulation also applies to other providers (providers of internet domain name and IP numbering services, such as IP address allocation and domain name registration services, providers of domain name registry services and providers of domain name-related privacy and proxy services), which are mentioned alongside specific information society services, but which are nevertheless also digital services. The necessary authority to process data is also established for these providers in § 24a.

Re Article 4 (Entry into force)

Re Paragraph 1

Article 4 stipulates in Paragraph 1 that the date of entry into force of the law is, in principle, the day after its promulgation.

Re Paragraph 2

Paragraph 2 provides for an exception for §§ 7 to 17, § 18(2), (3)(1)(b) and (2), as well as (4) to (7) and (8)(2) and § 19 in Article 1, which refer to Regulation (EU) 2023/1543 and will enter into force on 18 August 2026. The same principle applies to Article 3. This ensures that the implementing provisions of the Regulation do not apply before the Regulation itself has entered into force.