Processing status: February 7, 2024 3:20 p.m

Draft bill

of the Federal Ministry for Digital and Transport

Draft of a first law to amend the telecommunications Telemedia Data Protection Act

A. Problem and goal

Electronic communication via email, chat or messenger services and the use of cloud services are becoming increasingly important for private and professional exchange and storage of information compared to conventional number-based voice telephony. For number-independent interpersonal telecommunications services, secure end-to-end encryption is the industry standard. Suitable encryption technologies exist, but are not consistently provided by providers of these services.

The amendment to the Telecommunications Telemedia Data Protection Act (TTDSG) aims to oblige number-independent interpersonal telecommunications services to offer their telecommunications services as a standard with end-to-end encryption. The same applies to the storage of information when using cloud services, which are used by most commercial companies and an ever-increasing proportion of citizens. The right to encryption helps to increase acceptance of the widespread use of encryption technologies among the population, businesses and public institutions. It is an essential contribution to guaranteeing the fundamental rights to ensure telecommunications secrecy as well as the confidentiality and integrity of information technology systems and cybersecurity.

The draft law also serves to make clarifying and supplementary regulations in the area of supervision regulations by the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the Federal Network Agency (BNetzA) as well as the powers to process traffic, Location, inventory and usage data to fulfill the obligations under Regulation (EU) 2023/1543.

B. Solution

Insertion of a right to encryption in the Telecommunications Telemedia Data Protection Act.

C. Alternatives

No. A right to encryption requires legal regulation.

D. Household expenses excluding compliance costs

None.

E. Compliance Costs

E.1 Compliance costs for citizens

There are no compliance costs for citizens

E.2 Compliance costs for the economy

End-to-end encryption is already provided as standard by many affected service providers, so that a right to secure end-to-end encryption should not entail any significant compliance costs. In contrast, the economy attaches great importance to ensuring secure end-to-end encryption and sees this as a cornerstone of Germany as a business location.

Of which bureaucracy costs from information obligations

It is envisaged that the affected providers must inform their users about the implementation of end-to-end encryption or about how end-to-end encryption is made possible for users. In view of the already extensive user information provided by the providers, the effort associated with this information is likely to be low.

E.3 Administrative compliance costs

To be added: the BNetzA will have additional tasks in the area of supervision with regard to enabling end-to-end encryption by affected telecommunications providers.

F. Additional costs

Other costs for the economy, for social security systems, effects on individual prices and the price level, especially on the consumer price level, are not to be expected.

Draft bill of the Federal Ministry for Digital and Traffic

Draft of a first law to amend the telecommunications Telemedia Data Protection Act

From the ...

The Bundestag passed the following law:

Article 1

Amendment to the Telecommunications Telemedia Data Protection Act*)

The Telecommunications Telemedia Data Protection Act of June 23, 2021 (BGBl. I p. 1982; 2022 I p. 1045), which was last amended by Article 4 of the law of August 12, 2021 (BGBl. I p. 3544; 2022 I 1045) has been amended is amended as follows:

1. The table of contents is changed as follows:

a) After § 13 the following is added: “§ 13 a Fulfillment of obligations in accordance with Articles 10 and 11 of Regulation (EU) 2023/1543”.

b) After § 24 the following is added: “§ 24a Fulfillment of obligations in accordance with Articles 10 and 11 of Regulation (EU) 2023/1543”

2. The following numbers 7 and 8 are added to § 2 paragraph 2:

“7. “Secure end-to-end encryption” is an encryption technology through which telecommunications content is encrypted by the sending end user and only decrypted again by the receiving end user, so that it is unreadable over the entire transmission path and cannot be viewed and also by the provider -ter of the telecommunications service or third parties cannot access the key-

with.

8. “Participant data” means data in accordance with Article 3 number 9 of Regulation (EU) 2023/1543.”

3. The following paragraph 5 is added to § 3:

“(5) Providers of number-independent interpersonal telecommunications services within the meaning of Section 3 Number 40 of the Telecommunications Act carry out secure end-to-end encryption or ensure that end users provide their telecommunications content with end-to-end encryption can.

End users are responsible for implementing secure end-to-end encryption

*) The obligations arising from Directive EU/2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down an information procedure in the field of technical regulations and rules on information society services (OJ EC No. L 241 p. 1 dated September 17, 2015) have been observed.

by the provider of the telecommunications service or about how end-to-end encryption is possible. In the event that secure end-to-end encryption is not technically possible, the provider of the telecommunications service will provide information about the technical reasons that prevent secure end-to-end encryption."

4. After Section 13, the following Section 13a is inserted:

"§ 13a Fulfillment of obligations in accordance with Articles 10 and 11 of Regulation (EU) 2023/1543

Providers of commercially offered telecommunications services may process subscriber data, traffic data in accordance with Section 9 and location data in accordance with Section 13, to the extent that this is necessary to secure and transmit electronic evidence in the event of a European production order or to secure the data in the case of a European security order in accordance with Regulation (EU) 2023/1543 of the European Parliament and of the Council of July 12, 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings and for the enforcement of prison sentences following criminal proceedings is necessary.."

5. The following paragraph 6 is added to § 19:

"(6) "Providers of telemedia whose service consists of keeping information provided by the user of telemedia available for retrieval on a data storage device, inform the user about the possibility of continuous and secure encryption of the information provided, which ensures that the information can only be read by the user providing it."

6. After Section 24, the following Section 24a is inserted:

"§ 24a Fulfillment of obligations in accordance with Articles 10 and 11 of Regulation (EU) 2023/1543

Providers of commercially offered telemedia that enable their users to communicate with each other or to store or otherwise process data, provided that the storage of data is an integral part of the service provided to the user, as well as providers of Internet domain names and IP Numbering services such as IP address assignment and domain name registration services, providers of domain name registrar services and providers of data protection and proxy services associated with domain names may process subscriber data and usage data to the extent necessary to secure and transmit electronic evidence in the case of a European production order or to secure the data in the case of a European preservation order in accordance with Regulation (EU) 2023/1543 of the European Parliament and of the Council of July 12, 2023 on European production orders and European preservation orders for electronic evidence in criminal proceedings -driving and is necessary for the execution of prison sentences following criminal proceedings."

7. Section 28 is amended as follows:

a) In paragraph 1, the information "1." is replaced by the information "1a". The following number 1 is inserted before number "1a)":

"1. contrary to § 3 paragraph 5 sentences 2 and 3, the end user is not informed,"

b) In paragraph 1, the following number 10a is inserted after number 10:

“10a. contrary to § 19 paragraph 6, the user is not informed.

c) In paragraph 3, the information “numbers 1 and 9” is replaced by the information “numbers 1, 1a and 9” replaced.

8. Section 29 is amended as follows:

a) Paragraph 1 is worded as follows:

“The Federal Commissioner for Data Protection and Freedom of Information is the responsible supervisory authority for compliance with the legal requirements for the processing of participant data, traffic and location data according to §§ 9, 10, 12, 13 and 13a.”

b) In paragraph 2, the following is inserted after the word “telecommunications services”: “postal services”.

c) In paragraph 3 the following sentence is added:

“In particular, the Federal Commissioner for Data Protection and the Freedom of information

1. take orders and other measures to ensure compliance with data protection,

2. request information from the obligated party,

3. to check compliance with obligations, enter and inspect business and operational premises during normal operating or business hours,

4. in the event of non-fulfillment of data protection obligations, prohibit the operation of affected telecommunications systems or the provision of the relevant telecommunications service in whole or in part if milder interventions are not sufficient to enforce lawful behavior and

5. to enforce measures and orders according to numbers 1 to 4 in accordance with the Administrative Enforcement Act, set a penalty payment of up to 1 million euros."

9. The following paragraph 6 is added to § 30:

“(6) In order to enforce the ban according to § 8, the Federal Network Agency can request information about personal data from sellers and buyers from providers of online platforms that are used for trading in prohibited telecommunications systems, insofar as this is necessary for enforcement this law is necessary.”

Article 2

Entry into force, expiry

This law comes into force on April 1, 2025.

Reason

A. General part

I. Objective and necessity of the regulations

1. End-to-end encryption for number-independent interpersonal telecommunications services

Number-independent interpersonal telecommunications services, ie email services, messenger services and chat services, are now widely used in both private and professional areas. They are fully subject to the confidentiality of communication (EU level) and telecommunications secrecy in Germany.

While end-to-end encryption is not technically possible for number-based interpersonal telecommunications services (Section 3 Number 37 of the Telecommunications Act), end-to-end encryption is, to the extent that it is technically possible
number-independent interpersonal telecommunications services - in particular messenger services, a component of protecting the confidentiality of communication.
It serves to protect privacy as well as to protect professional and business secrets. End-to-end encryption secures encryption from end user to end user and prevents the provider or third parties from gaining knowledge of communication content on the servers that serve as intermediate stations during transmission. End users currently have no right to end-to-end encryption. Since end-to-end encryption is an existing technology to ensure the confidentiality of communication, it also serves the fundamental rights of telecommunications secrecy. End users should therefore have the right to use these services with end-to-end encryption, where technically possible.

On May 17, 2023, the Federal Cartel Office (BKartA) published its final report on the sector investigation into messenger and video services and placed a particular focus on data protection and data security issues - in particular on the topic of end-to-end encryption (see https://www.bundeskartell-amt.de/SharedDocs/Meldung/DE/Press Releases /2023/17_05_2023_SU_MD.html and https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektorprüfungen/Sek-torforschung_MessengerVideodienste. pdf;jsessio-nid=E4954BD5863FB199ED993B6FD2906D4E.1_cid381?__blob=publicationFile&v=5).

According to the findings from the BKartA's final report, the following picture emerges:

Although end-to-end encryption is now the industry standard, some messenger services do not use end-to-end encryption or only use it for certain functions, without technical restrictions justifying this.

In addition, the BKartA sees consumers being potentially misled by unclear information, such as whether end-to-end encryption is automatic, the end user has to activate it first, or whether it is limited to certain functions and what those are .

Technical limitations exist for video conferences and webinars because end-to-end encryption requires that participants are technically capable of providing and using the necessary encryption functions. According to the BKartA's findings, end-to-end encryption cannot be achieved

as soon as individual participants fall short of what is required
safety level lagging behind.

The BkartA also assumes that end-to-end encryption is not technically possible when using certain functions (participation via a number-based telecommunications service or recording of the conference by the service offering). According to the BKartA's findings, even when connecting devices that are based on the SIP protocol (Session Initiation Protocol - network protocol for setting up, controlling and terminating a communication session between two or more participants), it is end-to-end -Encryption is not possible because the various protocols would have to be synchronized.

Most other services that offer communication in groups cannot ensure end-to-end encryption because of the effort involved.

2. End-to-end encryption and interoperability

The BKartA does not see a technical approach for end-to-end encryption that is interoperable across the market. Interoperability is required by Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act) for certain services that are to be regarded as so-called “gatekeepers” according to the regulation. According to Article 2 number 29 of the Digital Markets Act, it means the ability to exchange information and to mutually use the information exchanged via interfaces or other solutions, so that all hardware or software components interact with other hardware and software in the intended manner function as intended for users. This is a challenge for end-to-end encryption and vice versa. The Digital Markets Act stipulates in Article 7 (Obligations of gatekeepers for the interoperability of number-independent interpersonal communications services) that the level of security, including end-to-end encryption, that the gatekeeper provides to its own end users: maintained across all interoperable services

must.

3. Encryption of information in cloud services

The right to secure and consistent encryption of information must also include information that is processed by users at external service providers for the user and which is only available there to authorized users and not to the public. The range of cloud services covers the entire spectrum of information technology and includes, among other things, infrastructure (e.g. computing power, storage space), platforms and applications. The right to encryption is regulated here for cloud services that function as storage services, which are increasingly used by most companies, but also by citizens, for example for back-up protection of communication content when using messenger services. Further services in the context of a cloud require special agreements between the user and the provider regarding encryption. This is not a telecommunications service, but a telemedia service to which telecommunications secrecy does not apply. To ensure data protection and cybersecurity, cloud service providers should ensure, as part of their technical and organizational precautions, that users of such services can protect the stored information with secure and consistent encryption. The right to encryption is an obligation of the provider to provide information, since the encryption is in the hands of the respective user.

4. Clarifications and additions in the area of supervision and regulations with regard to Regulation (EU) 2023/1543

In addition to the right to encryption, the draft law also serves to make clarifying and additional adjustments to the provisions on supervision by the BfDI and the Federal Network Agency. Furthermore, regulations are made that enable addressees of production and preservation orders for electronic evidence covered by the TTDSG to fulfill their obligations under Regulation (EU) 2023/1543 of the European Parliament and of the Council of July 12, 2023 European production orders and European preservation orders for electronic evidence in criminal proceedings and for the enforcement of prison sentences after criminal proceedings must be complied with.

men.

II. Essential content of the draft

The draft law includes a definition of end-to-end encryption, an addition to the principle of confidentiality of communication to include end-to-end encryption to be guaranteed, and an addition to the technical and organizational precautions with regard to the right to end -end-to-end encryption when using cloud services. Furthermore, the draft law largely contains clarifying and supplementary adjustments in the area of supervision by the BNetzA and BfDI. The draft law also contains the legal basis for processing traffic, location, inventory and usage data to fulfill the obligations under Regulation (EU) 2023/1543.

III. Alternatives

No.

IV. Legislative competence

The federal government's legislative competence with regard to the provisions on telecommunications data protection arises from its exclusive jurisdiction over telecommunications law (Article 73 Paragraph 1 Number 7 of the Basic Law). The regulation of data protection in the area of telemedia follows from the competing federal legislation on economic law (Article 74 paragraph 1 number 11 of the Basic Law).

IN. Compatibility with European Union law and international law contracts

There are no conflicting requirements under European Union law. The obligations arising from Directive EU/2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down an information procedure in the field of technical regulations and rules on information society services (OJ

EC No. L 241 p. 1 of September 17, 2015) have been observed.

WE. Legal consequences

1. Legal and administrative simplification

The draft law does not contain any regulations on legal and administrative simplification.

2. Sustainability aspects

Rules and indicators of the German sustainability strategy are not affected.

3. Household expenses without compliance costs

There are no household expenses without compliance costs.

4. Compliance costs

However, information obligations arise regarding end-to-end encryption
Affected providers must comply with the end users, although in view of the already extensive and constantly updated data protection information, no significant additional compliance effort is expected.

Furthermore, no significant compliance costs are expected from the implementation of the right to end-to-end encryption. In contrast, business attaches great importance to ensuring secure end-to-end encryption and sees this as a cornerstone of Germany as a business location.

End-to-end encryption is e.g. B. industry standard within messenger services, as the BKartA has determined. The regulation does not necessarily require services to make technical adjustments. At least for non-real-time-based communication (i.e. text messaging, email or file exchange), users are always able to use their own end-to-end encryption that is independent of the provider. The provider could therefore comply with the specifications without any need for adjustments, as long as it does not prevent this. There are no known affected services with technical configurations that actively prevent effective end-to-end encryption from being carried out. For other services the law depends

End-to-end encryption depends on it being technically possible, for example in the area of voice and video communication, especially when several people are involved (see the comments under I.).

5. Additional costs

Other costs for the economy, for social security systems, effects on individual prices and the price level, especially on the consumer price level, are not to be expected.

6. Further legal consequences

The improvement in the protection of the confidentiality of communication associated with a right to end-to-end encryption has a positive effect on the protection of privacy as well as professional and business secrets in electronic communication. The draft law has no impact on equality policy or demographics and does not affect the preservation and promotion of equal living conditions.

VII. time limit; Evaluation

No time limit or evaluation is provided.

B. Special part

Regarding Article 1 (Amendment to the Telecommunications Telemedia Data Protection Act)

To number 1

Number 1 contains the adjustments to the table of contents with regard to the insertion of new paragraphs into the TTDSG.

To number 2

Section 2 paragraph 2 number 7 defines the term secure end-to-end encryption. This occurs if the communication content remains encrypted throughout the entire transport route from end user to end user and cannot be viewed by the provider of the telecommunications service or third parties in between. Secure end-to-end encryption also implies that the key lies exclusively with the end user and that the provider of the telecommunications service cannot obtain it either. A distinction must be made between end-to-end encryption and transport encryption or point-to-point encryption, in which the communication content is unencrypted at the intermediate transmission stations such as the servers of the telecommunications providers and can be viewed by them or third parties.

Section 2 paragraph 2 number 8 defines the term participant data with reference to the in definition contained in Article 3(9) of Regulation (EU) 2023/1543. The definition is necessary in the TTDSG with regard to the authority to process data for the purpose of fulfilling obligations to release and preserve electronic evidence in accordance with Regulation (EU) 2023/1543. Data processing must be limited precisely to the area of personal data covered by the European production or preservation order.

To number 3

Section 3 paragraph 5 obliges providers of number-independent interpersonal telecommunications services to carry out secure end-to-end encryption or to ensure that end users can use these services with secure end-to-end encryption. This gives end users the right to end-to-end encryption of their communications as part of protecting the confidentiality of communications and telecommunications secrecy. End-to-end encryption protects the data packets to be transmitted in terms of confidentiality in such a way that the communication content is unreadable over the entire transmission path. This can only be guaranteed through secure end-to-end encryption, in which the data is encrypted when sent and only decrypted again at the recipient.

The regulation does not contain any direct obligation for the affected providers to arrange end-to-end encryption themselves. However, you must make this possible and may not take any technical or organizational measures that make it more difficult or prevent end users to use commonly used methods for consistent and secure end-to-end encryption. This reflects the current practice of providers, some of whom carry out end-to-end encryption themselves or leave activation to the end user. This practice is not affected by the right to encryption.

The right to end-to-end encryption is supplemented by the obligation to inform end users accordingly. The obligation to provide information counteracts the lack of transparency among consumers, which the BKartA identified in its final report on the sector investigation into messenger and video services. If end-to-end encryption is not possible for technical reasons, the provider will inform you

Telecommunications service informs the end user of the technical reasons that prevent end-to-end encryption.

A state of the art encryption method is not determined. The techniques currently used use an asymmetric encryption process that uses a key pair consisting of a public and a private key. The public key is used to encrypt the communication by the sending end user. This can then only be decrypted using the private key of the receiving end user.

To number 4

Number 4 contains a necessary regulation that legally enables commercially offered telecommunications services to process subscriber data (see number 2), traffic data and location data in order to fulfill their obligations under Regulation (EU) 2023/1543. In the context of criminal proceedings, the regulation regulates the release or preservation of electronic evidence by affected service providers on the basis of so-called “European production orders” or “European preservation orders” which are issued by the competent authorities in a member state. They can therefore require a service provider that offers services in the Union and has appointed a representative or designated a branch in another Member State to receive orders to hand over or secure electronic evidence, regardless of where the data is located condition.

Although Regulation (EU) 2023/1543 contains the obligation of the addressees to comply with such a production or preservation order, it does not contain any regulation that also authorizes the addressee to process personal data for this purpose. However, this is necessary in Germany with regard to the fundamental right to informational self-determination and to maintain telecommunications secrecy.

Following the image of a double door, the legislature must create proportionate legal bases for both the transmission of personal data by telecommunications providers and for the retrieval of this data by the authorities. Transmission and retrieval regulations must sufficiently limit the purposes for which the data is used, in particular by providing for factual intervention thresholds and sufficiently important protection of legal interests (cf. BVerfG decision of May 27, 2020 - 1 BvR 1873/13, 1 BvR 2618/13 (Inventory data information II). The TTDSG does not yet contain any regulation that authorizes affected service providers to process traffic or location data for the purposes of the European production or preservation order. The TTDSG would therefore support the release and preservation of electronic evidence without such a regulation which involves the processing of traffic or location data, without such a regulation.

According to Article 3(8) of this Regulation, electronic evidence means subscriber data, traffic data or content data stored by or on behalf of a service provider at the time of receipt of a European Production Order Certificate or a European Preservation Order Certificate. Traffic and content data according to Regulation (EU) 2023/1543 (Article 3 Numbers 11 and 12) correspond to the traffic and location data of the TTDSG. According to the TTDSG, traffic data includes both the content data and the metadata such as the origin and destination of a message, data about the location of the device, date, time, duration, size, route, format, protocol used and type of compression. The addressees of a European production order and a European preservation order are service providers, which include electronic communications services within the meaning of Article 2 number 4 of Directive (EU) 2018/1972 (Article 3 number 3 letter a of Regulation (EU) 2023/1543). As a rule, these are paid-for services, ie commercially provided Internet access services, interpersonal communication services (both number-based and number-independent) and services that are wholly or predominantly in the

Transmission of signals exists, such as transmission services used for machine-machine communication and for broadcasting. Telecommunications services provided purely for business purposes, which are not provided commercially, i.e. without being part of an economic consideration, such as the provision of telecommunications within companies or other organizations as part of employment or service relationships, are not subject to any surrender or security order therefore do not require any authorization to process traffic or location data.

To number 5

In Section 19 Paragraph 6 there is an obligation to provide information regarding the possibilities of a secure and end-to-end encryption of the information provided when using cloud storage was introduced. Cloud services are telemedia that consist of storing information provided by a user for the user. The use of cloud services to store private and corporate data is becoming increasingly widespread. The secure and continuous encryption of information on cloud storage is technically possible and serves data security in terms of protection against cyber attacks in general and the protection of personal data in particular. Most companies now use cloud services to relocate storage space, computing capacity or software applications to external servers.

In addition, an ever-increasing proportion of citizens are using cloud services, for example for backing up messages on messenger services. Consistent and secure encryption of information in the cloud, which ensures that this information can only be read by the user providing it, is just as important as when using number-independent interpersonal telecommunications services. Therefore, cloud storage providers should inform

ren.

To number 6

As in number 4, the telemedia providers affected by Regulation (EU) 2023/1543 also require a special legal basis for processing subscriber and usage data, without which a European production or preservation order addressed to these providers would be ineffective. The TTDSG has regulated the provision of information about inventory and usage data within narrow limits in Sections 21-24. It does not contain powers to process data for the purpose of securing and transmitting electronic evidence on the basis of a European production or preservation order. The new Section 24a closes this gap. Regulation (EU) 2023/1543 does not affect all telemedia providers (in the regulation, information society services within the meaning of Article 1 paragraph 1 letter b of Directive (EU) 2015/1535), but only the commercial providers of telemedia which enable their users to communicate with each other or to store or otherwise process data, provided that the storage of data is an integral part of the service provided to the user. Accordingly, the necessary authority to process data must be limited to these providers. Telemedia providers 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 online gaming platforms and online gambling. This does not include telemedia that does not enable its users to communicate with each other, but only offers communication with the service provider. This also does not include telemedia that does not enable its users to store or otherwise process data, or if data storage is not a determining, i.e. not an essential, part of the service provided to the user, as in the case of legal services provided online, Architectural, engineering and accounting services (Recital 27 of Regulation (EU) 2023/1543). The regulation also affects other providers (providers of Internet domain names and IP numbering services such as IP numbering services).

address assignment and domain name registration, providers of domain name registrar services and providers of data protection and proxy services associated with domain names), which are mentioned in addition to the specific information society services, but which are nevertheless also telemedia. The necessary authority to process data for these providers is also regulated in Section 24a.

To number 7

The changes in § 28 impose a fine on the obligation to provide information about end-to-end encryption in accordance with § 3 paragraph 5, which is supervised by the Federal Network Agency. Furthermore, a fine will be imposed if cloud services do not meet the requirements of Section 19 Paragraph 6.

To number 8

Regarding letter a

The new version of Section 29 paragraph 1 serves to clarify the supervisory responsibility of the BfDI. This® is responsible for compliance with the legal requirements for the processing of personal data by telecommunications companies, as they arise from the GDPR and, with regard to the permitted processing of traffic and location data, specifically from the TTDSG. The responsibility of the BfDI with regard to compliance with the general data protection provisions of the GDPR is regulated in Section 9 Paragraph 1 of the Federal Data Protection Act and does not need to be repeated here. The supervision of the BfDI refers to the special permissions regulated in the TTDSG for the processing of traffic data in Sections 9, 10, 12 and for the processing of location data in Section 13. The clarification corresponds to the regulation on responsibility for fines in Section 28 TTDSG and serves to coordinate more precisely with the supervisory responsibility of the BNetzA, which according to Section 30 is the responsible supervisory authority for all other provisions of Part 2 of the TTDSG.

Regarding letter b

The addition in paragraph 2 also assigns the BfDI supervision with regard to postal services accessing the end user's terminal equipment. Like telecommunications services, postal services are subject to supervision by the BfDI.

Regarding letter c

The addition in paragraph 3 aims to make it clear that the BfDI has no lesser powers than the BNetzA in accordance with Section 30 when carrying out its tasks.

To number 9

The addition of a new paragraph 6 to § 30 serves to close a legal gap in the enforcement of the ban according to § 8. In the context of online trading in telecommunications systems prohibited under § 8, operators of online platforms used for this purpose are currently not authorized to inform the Federal Network Agency to provide information about personal data of sellers and buyers because there is no legal obligation to do so and accordingly no right under Article 6 paragraph 1 letter c of Regulation (EU) 2016/679 (General Data Protection Regulation) to process personal data for this purpose. The Federal Network Agency therefore currently has no way of identifying owners of prohibited telecommunications systems and taking action against ownership if the telecommunications systems in question were purchased via online sales platforms.

Regarding Article 2 (entry into force, expiry)

Article 2 sets the entry into force on April 1, 2025.