Draft Act

of the Federal Government

Draft Act transposing the NIS 2 Directive and regulating essential features of information security management in the federal administration

(NIS 2 Transposition and Cybersecurity Enhancement Act)

A. Problem and objective

Germany’s modern economy depends on well-functioning and resilient infrastructure, both physical and digital, for its functioning, generating prosperity and growth, and also for its adaptability to changing economic policy and geopolitical framework conditions. These factors have significantly grown in importance in recent years. Companies face a variety of challenges not only in their economic activities, but also in their practical security. European-wide and globally interconnected processes, as well as the increasing digitalisation of all areas of life, and thus also of the economy, are leading to greater vulnerability to external, often non-controllable factors. Information technology plays a central role in critical installations as well as in certain companies. Their security and resilience form also the basis for security of supply, from the supply of electricity and water to the disposal of municipal waste. The same applies to the functioning of the market economy in Germany and the internal market of the European Union. The interconnectedness and close integration of the economy within Germany and the European Union is the result of interdependencies in cybersecurity. In this context, the increased cybersecurity requirements for legal and natural persons providing essential services or carrying out activities are set out in Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80; ‘NIS 2 Directive’) further aligned across the European Union.

In its 2023 report on the state of IT security in Germany, the Federal Office for Information Security (BSI) estimates that the overall IT security situation has worsened as a result of Russia's war of aggression against Ukraine, which violates international law. In the field of business, ransomware attacks, exploitation of vulnerabilities, open or incorrectly configured online servers as well as dependencies on the IT supply chain and, in this context, cyberattacks via the supply chain (so-called supply chain attacks) are among the greatest threats. In addition to the already known threats, the Russia's war of aggression against Ukraine and the resulting ‘turning point’ also gave rise to new threats or the assessments of already known threats had to be changed due to changing framework conditions. Examples of this are in the field of hacktivism, in particular through distributed denial of service (DDoS) attacks or collateral damage caused in Germany as a result of cyber sabotage attacks in the context of the war. In addition, supply chain disruptions and attacks, both in the areas of cybercrime and war, have also increased recently. These phenomena are no longer occurring only occasionally, but have become part of everyday business life. Increasing the resilience of the economy to the dangers of the digital world is therefore a key task for the players involved in the state, economy and society in order to maintain Germany’s and the European Union’s internal market as a whole robust, efficient and functional as a business location.

For information security management in the federal administration, the previous governance tools have proven to be insufficiently effective on a predominantly sub-statutory ba-

sis to achieve a comprehensively effective increase in the level of security. This has been confirmed, in particular, by surveys on the current status of the Federal implementation plan and audits carried out by the Federal Court of Auditors (BRH). Against the backdrop of the current geopolitical developments (‘turning point’), the threat situation has once again intensified, further increasing the risk of governmental entities being restricted in their ability to act by threats from cyberspace.

This draft is in the context of the efforts of the European Union and its Member States to increase economic security and enhance resilience in response to a new geopolitical framework conditions. With the European Economic Security Strategy, published on 20 June 2023, the European Commission identifies the risk to the security of critical infrastructure from physical and cyberattacks as one of four main risks for the European economy.

This draft is also in the context of the jeopardised timely achievement of the goals of the United Nations General Assembly resolution of 25 September 2015 entitled ‘Transforming our world: the UN 2030 Agenda for Sustainable Development’. In particular, the draft aims to contribute to the achievement of Sustainable Development Goal 9 of the UN 2030 Agenda to build high-quality, reliable and resilient infrastructure.

B. Solution, benefits

In accordance with the requirements of EU law, the regulatory framework established by the Act on Increasing the Security of Information Technology Systems (IT Security Act) of 17 July 2015 (Federal Law Gazette (BGBl.) I 2015, p. 1324) and the Second Act on the Enhancement of the Security of Information Technology Systems (IT Security Act 2.0) of 18 May 2021 (Federal Law Gazette (BGBl.) I 2021, p. 1122) is extended to the area of certain undertakings by the NIS 2 Transposition and Cybersecurity Enhancement Act; in addition, corresponding requirements for the federal administration are introduced. The main amendments are as follows:

– Introducing the categories of entities specified by the NIS 2 Directive, accompanied by a significant expansion of the scope of application previously limited to operators of critical infrastructures, providers of digital services and companies in the special public interest.

– The catalogue of minimum security requirements of Article 21(2) of the NIS 2 Directive is incorporated into the BSI Act, distinguishing between categories in the intensity of the measure in question for reasons of proportionality.

– The previous one-stage incident reporting obligation will be replaced by the three-stage reporting regime of the NIS 2 Directive. The aim is to minimise the bureaucratic burden on entities within the existing scope for implementation by Member States.

– Extending the tools of the Federal Office for Information Security (BSI) with regard to supervisory measures prescribed by the NIS 2 Directive.

– Legally enshrining essential national requirements for federal information security management and mapping the associated roles and responsibilities.

– Harmonising requirements for Federal Administration entities arising from national and EU legislation in order to ensure a coherent and manageable regulatory regime overall.

– Establishing a federal CISO as the central coordinator for information security measures in Federal Administration entities and to assist the departments in implementing the information security management requirements.

The NIS 2 Directive aims to introduce mandatory administrative and business measures to ensure a high common level of cybersecurity across the European Union. Important and particularly important institutions are to be protected from damage caused by cyberattacks and the functioning of the European internal market is to be improved. The consequences of a cyberattack are very diverse and cannot be fully quantified. For example, ransomware attacks can encrypt the servers of medical facilities, preventing the admission of new emergencies and outpatient care for days. These are, for example, risks and threats to the life and limb of the population, which cannot be expressed in monetary terms. In terms of the quantifiable damage directly caused to businesses in Germany as a result of cyberattacks, the Association of German Information and Telecommunications Companies (Bitkom e.V.) estimates a total annual damage of around EUR 223.5 billion for 2021. In 2022, the total damage volume amounted to EUR 202.7 billion and is expected to be EUR 205.9 billion in 2023. On average, cyberattacks have caused a total annual damage to businesses in Germany of around EUR 210.7 billion over the last three years. Bitkom surveyed German businesses with at least 10 employees and an annual turnover of at least one million euros. A total of around 3.4 million legal entities were registered in the Federal Statistical Office's business register in the 2021 reporting year, of which 444,055 legal entities had at least 10 employees. Assuming an equal distribution of the total damage volume among businesses with a least 10 employees, the damage volume per business would be around EUR 500,000 (= EUR 210.7 billion/444,055 companies). It can be assumed that even if the security standards specified by the NIS 2 Directive are fully implemented, not all damage caused by cyberattacks can be averted. If, however, it is assumed that the implementation of the present requirements will make it possible to offset half of the annual damage caused to the businesses obliged to implement the NIS 2 Directive, then there will be around EUR 250,000 per business. Extrapolated to the estimated number of businesses concerned, this means a total damage to the German economy of approximately EUR 3.6 billion (= EUR 250,000 * 14,500 businesses). In addition to the estimated damage to businesses of around 3.6 billion, the damage to public administration that cannot be quantified in the absence of available data must also be taken into account, as well as other damage.

C. Alternatives

None.

D. Budgetary expenditure exclusive of compliance costs

For the federal budget, the Act will result in one-off expenditure of around EUR 38.2 million for the federal administration and total current annual expenditure of around EUR 772.32 million until 2029. The one-off expenditure includes the material costs for the years 2026 to 2029. The breakdown of one-off and current annual expenditure between 2026 and 2029 is as follows:

	2026	**2027**	**2028**	**2029**
one-off expenditure (in million euros)	36.87	1.17	0.086	0.077
current expenditure (in million euros)	155.49	190.98	209.64	216.21
Expenditure (total, in million euros)	**192.36**	**192.16**	**209.73**	**216.28**

The need for material and personnel resources as well as positions and posts should be balanced financially and in terms of posts in the relevant section of the budget. This also applies to the compliance costs presented under E.3, insofar as these have an impact on the budget.

There is no additional expenditure for Länder and municipalities.

The Act generates a total of current annual expenditure for social security institutions of around EUR 16.9 million.

E. Compliance costs

E.1 Compliance costs for citizens

No compliance costs will arise for citizens.

E.2 Compliance costs for businesses

For businesses, annual compliance costs will rise by around EUR 2.2 billion. In total, one-off expenditure of around EUR 2.1 billion will be incurred. This is almost exclusively assigned to this category

Introduction or adaptation of digital process flows

.

Administrative costs under this heading arising from information obligations

Approximately EUR 1.9 million is spent on administrative costs resulting from information obligations.

E.3 Compliance costs for the authorities

For the federal administration, annual compliance costs will rise by EUR 122.28 million. The one-off compliance costs amount to EUR 38.21 million. The annual compliance costs of the Länder will rise by EUR 85,000.

F. Other costs

None.

Draft Act of the Federal Government

Draft law transposing the NIS 2 Directive and regulating essential features of information security management in the federal administration

(NIS 2 Transposition and Cybersecurity Enhancement Act) *) 1)

From the...

The Bundestag has adopted the following act:

Contents overview

---

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).

) This Act serve to transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80).

Article 1

Act on the Federal Office for Information Security and on Information Technology Security of Entities

(BSI Act – BSIG)

Table of contents

Part 2
The Federal Office

Chapter 1
Tasks and powers

Chapter 2
Data processing

Part 3
Security in the information technology of entities

Chapter 1
Scope of application

Chapter 2
Risk management, reporting, registration, demonstration and information obligations

Chapter 3
Information security of federal administrative entities

Part 4
Domain Name Registration Data Databases

Part 1

General Provisions

§ 1

Federal Office for Information Security

The Federal Office for Information Security (the Federal Office) is a higher federal authority within the remit of the Federal Ministry of the Interior and Community. It is the central body for information security at national level. The Federal Office carries out tasks vis-à-vis the federal ministries on the basis of scientific and technical knowledge.

§ 2

Definitions

In accordance with this Act, the following terms shall be defined as follows:

1. ‘near miss’ means an event that could have affected the availability, integrity or confidentiality of stored, transmitted or processed data or the services offered or accessible via information technology systems, components and processes, but whose occurrence was successfully prevented or did not occur for other reasons;

2. ‘legitimate access seekers’ means

   a) the Federal Office,

   b) the Land authorities designated by the Länder as competent authorities for the supervision of public administration entities at regional level under Article 2(2)(f)(ii) of the NIS 2 Directive,

   c) law enforcement authorities,

   d) the Federal and Länder police, and

   e) the Federal and Länder constitutional protection authorities;

3. ‘ground-based infrastructure’ means facilities relating to the space sector which are used to control the launch, flight or eventual landing of space objects;

4. ‘cloud computing service’ means a digital service that enables the on-demand management of a scalable and elastic pool of shared computing resources, as well as extensive remote access to that pool, even if the computing resources are distributed across multiple locations;

5. ‘Content Delivery Network’ or ‘CDN’ means a group of geographically distributed interconnected servers, together with the necessary infrastructure connected to the internet, and the provision of digital content and services to internet users on behalf of content and service providers, with the aim of ensuring high availability, accessibility or delivery with the lowest possible latency;

6. ‘cyber threat’ means a cyber threat as defined in Article 2 point (8) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA

(the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act, OJ L 151, 7.6.2019, p. 15);

7. ‘data traffic’ means data transmitted by means of technical protocols; telecommunications content pursuant to Section 3(1) of the Telecommunications Digital Services Data Protection Act and usage data pursuant to Section 2(2)(3) of the Telecommunications Digital Services Data Protection Act may be included;

8. ‘DNS service provider’ means a natural or legal person who:

   a) provides publicly available recursive domain name resolution services to internet end-users; or

   b) provides authoritative domain name resolution services for use by third parties, with the exception of root name servers;

9. ‘domain name registry service provider’ means a registrar or an entity acting on behalf of registrars, in particular providers or resellers of data protection or proxy registration services;

10. ‘significant cyber threat’ means a cyber threat that has the potential to significantly affect the information technology systems, components and processes due to the specific technical characteristics of the cyber threat; an adverse effect is significant if it is likely to cause significant material or non-material damage;

11. ‘significant security incident’ means an security incident which:

    a) has caused or is likely to cause serious disruption to the operation of services or financial loss to the entity concerned; or

    b) has affected or is likely to affect other natural or legal persons by causing substantial material or non-material damage;

    unless a more specific definition is provided by the statutory order pursuant to Section 56 (5);

12. ‘research entity’ means an entity whose primary objective is to carry out applied research or experimental development with a view to exploiting the results of that research for commercial purposes; educational establishments are not considered as research entities;

13. ‘senior management’ a natural person appointed by law, statutes or articles of association to conduct the business and to represent a particularly important or important entity; heads of federal administration entities according to Section 29 are not considered to be senior management;

14. ‘ICT service’ means an ICT service as defined in Article 2 point (13) of Regulation (EU) 2019/881;

15. ‘ICT product’ means an ICT product as defined in Article 2 point (12) of Regulation (EU) 2019/881;

16. ‘ICT process’ means an ICT process as defined in Article 2 point (14) of Regulation (EU) 2019/881;

17. ‘;information security’ means the adequate protection of the confidentiality, integrity and availability of information;

18. ‘information technology’ means a technical means of processing information;

19. ‘social security institutions’ means corporations within the meaning of Section 29 of the Fourth Book of the Social Security Code, working groups as defined in Section 94 of the Tenth Book of the Social Security Code, the German Statutory Accident Insurance (Deutsche Gesetzliche Unfallversicherung e.V.) and Deutsche Post AG, in so far as it is responsible for calculating or paying social benefits;

20. ‘Internet Exchange Point’ or ‘IXP’ means an infrastructure which:

    a) enables the interconnection of more than two independent autonomous systems primarily used for the exchange of Internet traffic;

    b) only serves the interconnection of autonomous systems; and

    c) does not require that:

        a%6) the internet data traffic between any two participating autonomous systems runs through a third autonomous system; or

        b%6) alters or otherwise impairs the data traffic related to it;

21. ‘federal communications technology means information technology operated by one or more federal administrative entities or on behalf of one or more federal administration entities, for the purpose of communication or exchange of data within a federal administration entity, of federal administration entities between themselves or of federal administrative entities with third parties; the communications technology of the Federal Constitutional Court, the federal courts, in so far as they do not perform administrative tasks under public law, the Bundestag, the Bundesrat, the Federal President and the Federal Court of Auditors, in so far as they have exclusive responsibility for its operation, are not considered as ‘federal communications technology’;

22. ‘critical assets’ means a facility that is essential for the provision of a critical service; critical assets within the meaning of this Act shall be determined in more detail by the statutory ordinance pursuant to: Section 56(4);

23. ‘critical components’ means ICT products,

    a) which are used in critical assets,

    b) in which disruptions to availability, integrity and confidentiality can lead to a failure or significant impairment of the functioning of critical assets or to threats to public security; and

    c) which are designated

        a%6) as critical components on the basis of a law with reference to this provision; or

        b%6) realise a function determined as critical on the basis of a law;

    if no critical components and no critical functions from which critical components can be derived are determined by law with reference to this provision for one of the sectors referred to in subparagraph 24, there are no critical components in that sector within the meaning of this subparagraph;

24. ‘critical service’ means a service for the supply of the general public in the sectors of energy, transport and traffic, finance, social security institutions and basic security for

job seekers, healthcare, water, food, information technology and telecommunications, space or municipal waste disposal, the failure or impairment of which would lead to significant supply shortages or threats to public safety;

25. ‘Managed Security Service Provider’ or ‘MSSP’ means an MSP that implements or provides support for cybersecurity risk management activities;

26. ‘Managed service provider’ or ‘MSP’ means a provider of services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, through support or active management at customers’ premises or remotely;

27. ‘NIS 2 Directive’ means Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80), as amended;

28. ‘online marketplace’ means a service within the meaning of Section 312l(3) of the Civil Code;

29. ‘online search engine’ means a digital service as defined in Article 2 point (5) of 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 (OJ L 186, 11.7.2019, p. 57);

30. ‘social networking platform’ means a platform where end users can contact and communicate with each other, in particular through chats, posts, videos and recommendations, using different devices, and share and discover content;

31. ‘log data’ means control data of an information technology protocol used for the transmission of data which:

    a) are necessary to ensure communication between receiver and transmitter; and

    b) are transmitted independently of the content of the communication process or stored on the servers involved in the communication process;

    log data may contain traffic data pursuant to Section 3 point (70) of the Telecommunications Act and usage data pursuant to Section 2(2)(3) of the Telecommunications Digital Services Data Protection Act;

32. ‘logging data’ means records of technical events or conditions within information technology systems;

33. ‘qualified trust service’ means a qualified trust service as defined in Article 3 point (17) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73);

34. ‘qualified trust service provider’ means a qualified trust service provider as defined in Article 3 point (20) of Regulation (EU) No 910/2014;

35. ‘data centre service’ means a service consisting of structures that serve the primary purpose of centrally hosting, interconnecting and operating IT or network equipment, and which provide data processing services, including all necessary facilities and infrastructures, in particular for power distribution and environmental control;

36. ‘malware’ means programmes and other information technology routines and procedures used to use or erase data without authorisation or to influence other information technology processes without authorisation;

37. ‘federal communications technology interfaces’ means security-related gateways within the federal communication technology and between it and the information technology of individual federal administration entities, groups of federal administration entities or third party information technology; the components at the network gateways which are operated under the responsibility of the courts and constitutional bodies referred to in subparagraph 21 are not considered to be federal communications technology interfaces;

38. ‘vulnerability’ means a characteristic of ICT products or services that can be exploited by third parties to gain access to the ICT products or ICT services contrary to the wishes of the party so entitled, or to influence the functioning of the ICT products or ICT services;

39. ‘security in information technology’ means compliance with certain security standards relating to the availability, integrity or confidentiality of information by means of security measures;

    a) in information technology systems, components or processes or

    b) in the application of information technology systems, components or processes;

40. ‘security incident’ means an event affecting the availability, integrity or confidentiality of stored, transmitted or processed data or of the services offered or accessible through information technology systems, components and processes;

41. ‘systems for detecting attacks’ means processes supported by technical tools and organisational involvement to detect attacks against information technology systems; the detection of an attack shall be carried out by comparing the data processed in an information technology system with information and technical patterns indicating attacks;

42. ‘Top Level Domain Name Registry’ means a natural or legal person who manages and operates the registration of Internet domain names within a specific Top Level Domain (TLD), including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files through the name servers, whether the operation is carried out or outsourced by the natural or legal person itself; no Top Level Domain Name Registries are registries that uses TLD names for their own purposes only;

43. ‘trust service’ means a trust service as defined in Article 3 point (16) of Regulation (EU) No 910/2014;

44. ‘trust service provider’ means a trust service provider as defined in Article 3 point (19) of Regulation (EU) No 910/2014;

45. ‘space-based services’ means services relating to the space sector that are based on data and information either generated by or transmitted through space assets, the disruption of which may lead to wider cascading effects that may have far-reaching and long-lasting negative impacts on the provision of services across the internal market;

46. ‘certification’ means the determination by a certification body that a product, a process, a system, a protection profile (security certification), an individual (personal certification) or an IT security service provider meets certain requirements.

Part 2

The Federal Office

Chapter 1

Tasks and powers

§ 3

Tasks of the Federal Office

(1) The Federal Office shall promote the security in information technology. To this end, it performs the following important tasks in the public interest:

1. avert threats to the security of federal information technology;

2. gather and evaluate information on security risks and security precautions and make the lessons learned available to other entities to the extent necessary for the performance of their tasks and make them available to third parties to the extent necessary to safeguard their security interests;

3. carry out tasks within the Cooperation Group and the CSIRTs network in accordance with Articles 14 and 15 of the NIS 2 Directive;

4. investigate security risks in the use of information technology and develop security measures, in particular information technology procedures and devices for security in information technology (IT security products), to the extent necessary for the fulfilment of Federation's tasks, including research within the scope of its statutory tasks;

5. develop criteria, procedures and tools for testing and assessing the security of information technology systems or components and for testing and assessing conformity in the area of IT security;

6. carry out peer reviews in accordance with Article 19 of the NIS 2 Directive;

7. establish security requirements for the communication infrastructure of inter-ministerial communications networks and other federal communications infrastructures in consultation with the relevant operators and verify compliance with these security requirements;

8. examine and evaluate the security of information technology systems or components and issue security certificates;

9. perform tasks and exercise powers referred to in Article 58(7) and (8) of Regulation (EU) 2019/881 as the national authority for the cybersecurity certification;

10. check and confirm conformity in the area of IT security of information technology systems and components with technical guidelines issued by the Federal Office;

11. examine, assess and authorise information technology systems or components used for the processing of officially classified information pursuant to Section 4 of the Secu-

rity Clearance Check Act in the area of the Federal Government or by businesses in the context of federal contracts;

12. produce key data and operate cryptography and security management systems for federal information security systems used to protect official confidentiality or in other areas at the request of the authorities concerned;

13. provide support and advice on organisational and technical security measures and carry out technical tests to protect confidential official information in accordance with Section 4 of the Security Clearance Check Act against unauthorised access;

14. develop technical security standards for federal information technology to be used and for the suitability of contractors in the area of federal information technology in special need of protection;

15. make IT security products and IT security services available to federal administration entities;

16. provide support for the federal bodies responsible for the security of information technology, especially where these bodies undertake advisory or supervisory tasks; this shall apply, as a priority, to the Federal Commissioner for Data Protection and Freedom of Information, whose support is provided within the framework of the independence he or she performs his or her tasks under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1; L 314, 22.11.2016, p. 72; L 127, 23.5.2018, p. 2 and under the Federal Data Protection Act;

17. advise and support federal administration entities on information security issues, including the handling of security incidents, and provide specific, practical tools for implementing information security requirements, in particular for implementing the requirements under Section 30 and Section 44;

18. provide support

    a) for the federal police and law enforcement authorities in carrying out their statutory tasks;

    b) of the Federal Office for the Protection of the Constitution and the Military Counter-Intelligence Service in the evaluation and assessment of information arising from the observation of endeavours directed against the free basic democratic order, the existence of the State or the security of the Federation or a Land, or arising from the observation of security-threatening or secret service activities within the scope of the statutory powers under the Federal Constitution Protection Act or the MAD Act,

    c) of the Federal Intelligence Service in carrying out its statutory tasks;

    support must only be provided to the extent required to prevent or investigate activities which are targeted against the security in the information technology or which are carried out by using the information technology. The support requests are to be documented by the Federal Office;

19. support the competent bodies of the Länder, at their request, in matters relating to the prevention of threats to information technology security;

20. advise, inform and warn federal administration entities as well as manufacturers, distributors and users on information technology security issues, particularly with regard to the possible consequences of missing or inadequate security precautions;

21. pprotecting and informing consumers in the field of information technology security, in particular advising and alerting consumers on information technology security issues, with regard to the possible consequences of missing or inadequate security precautions;

22. create appropriate communications structures to recognise crises at an early stage, respond and manage crises and to coordinate efforts to protect critical information infrastructures in cooperation with private industry.

23. performing tasks as a central body in the field of information technology security with a view to cooperating with the competent bodies abroad, without prejudice to the specific responsibilities of other bodies;

24. performing tasks in accordance with Section 40 as the central body for the security of information technology of particularly important entities and important entities, including requesting and providing administrative assistance in accordance with Article 37 of the NIS 2 Directive;

25. support the restoration of the security or the functioning of information technology systems in exceptional cases in accordance with Section 11;

26. develop recommendations for identification and authentication procedures and assess them with regard to information security;

27. describe and publish a state of the art of security requirements for IT products, taking into account existing norms and standards and involving the business associations concerned;

28. co-operate with national computer emergency response teams of third countries or equivalent bodies of third countries and support these teams or bodies; deployments of the Federal Office in third countries may not be carried out against the will of the State on whose territory the measure is to take place; the decision on the deployment of the Federal Office in third countries is taken by the Federal Ministry of the Interior and Community in agreement with the Federal Foreign Office;

29. cooperate with the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht) and exchange information to the extent necessary for the performance of its tasks, in particular with regard to the measures taken pursuant to Regulation (EU) 2022/2554; the Federal Financial Supervisory Authority shall provide the Federal Office with the information necessary for the performance of its tasks.

(2) the Federal Office may, upon request, support the Länder in securing their information technology.

(3) the Federal Office may, at their request, advise and support particularly important entities in securing their information technology or refer them to qualified security service providers.

§ 4

Federal Financial Intelligence Unit for Information Technology Security

(1) The Federal Office is the Financial Intelligence Unit for cooperation among federal administrative entities in matters relating to security in information technology.

(2) To perform this task, the Federal Office shall:

1. gather and evaluate information necessary for the prevention of threats to information technology security, in particular on vulnerabilities, malware, attacks or attempted attacks on information technology security and the practices observed;

2. inform the federal administration entities without delay about information as referred to in subparagraph 1 concerning them and of the facts of the matter ascertained,

3. provide federal administration entities with recommendations on how to deal with the risks.

(3) An exception to the reporting requirements under paragraph 2 subparagraph 2 shall be made for information which may not be disclosed due to confidentiality regulations or agreements with third parties, and for information whose disclosure would conflict with the constitutional status of a member of the German Bundestag or of a constitutional body, or with the legally mandated autonomy of individual bodies.

§ 5

General Reporting Centre for Information Technology Security

(1) In order to perform the tasks under Section 3, the Federal Office, as the central body for reporting from third parties, shall receive information on security risks in information technology and analyse that information. The Federal Office is the national coordinator for the purposes of coordinated vulnerability disclosure under Article 12(1) of the NIS 2 Directive.

(2) In order to perform its tasks under paragraph 1, the Federal Office shall receive information on vulnerabilities, malware, attacks or attempted attacks on information technology security and the practices observed, as well as on security incidents, cyber threats and near misses. The Federal Office shall set up appropriate reporting tools for this purpose. Reports can be made anonymously. If the report is not made anonymously, the reporter may, at the time of the report or later, request that his or her personal data be disclosed only in anonymised form. This shall not apply in the cases of: Section 8(6) and (7), first sentence. A transfer of personal data in the cases of: Section 8(6) and (7), first sentence shall nottake place if it is apparent to the Federal Office that the interests of the reporter worthy of protection outweigh the general interest in the transfer. The manner in which the reporter obtained the information must also be taken into account. The decision pursuant to sentence 6 must be submitted for prior examination to the official data protection officer of the Federal Office and to another employee of the Federal Office who is qualified to hold judicial office.

(3) The Federal Office shall use the information reported in accordance with paragraph 2 to:

1. inform third parties about any known vulnerabilities, malware or attempted attacks on information technology security to the extent necessary for the protection of their security interests;

2. warn and inform the public or interested parties in accordance with Section 13;

3. inform federal administration entities in accordance with Section 4(2)(2) of the information concerning them;

4. inform particularly important and important entities as defined in: Section 40(3)(4)(a) of the information concerning them;

5. carry out its tasks as competent authority, CSIRT and single point of contact within the meaning of the NIS 2 Directive.

(4) Disclosure in accordance with paragraph 3, subparagraphs 1, 2 or 4 shall not take place to the extent that the information reported in accordance with paragraph 2:

1. include trade and business secrets of third parties and the measures taken in accordance with: paragraph 3 cannot be carried out without disclosing of those trade and business secrets; or

2. may not be transmitted on the basis of agreements between the Federal Office and third parties.

(5) Other statutory reporting obligations, regulations on the protection of secrets, statutory obstacles to transmission and transmission regulations shall remain unaffected.

§ 6

Information exchange

(1) The Federal Office operates an online platform for the exchange of information with important entities, particularly important entities and entities of the federal administration. It can involve the participating manufacturers, suppliers or service providers to exchange information on cyber threats, vulnerabilities, near misses and IT security measures, as well as to detect and counter cyberattacks. The Federal Office may allow other bodies to participate.

(2) The Federal Office specifies conditions of participation for the exchange of information and the use of the platform between participants.

§ 7

Control of federal communications technology, rights of access

(1) The Federal Office is authorised to control the security of the federal communications technology and its components, including technical infrastructures required for the operation of federal communications technology. To this end, it may

1. demand the provision of the information required carrying out the tasks under: Section 3(1), sentence 2, subparagraphs 1 and 20, in particular on technical details, on strategies, plans and regulations relating to the federal communication technology, including structure and process organisation; and

2. inspect documents and data carriers of the operator of the relevant federal communications technology or of a third party commissioned to provide operating services and demand that copies of these documents and records, including in electronic form, be

handed over free of charge, provided this does not conflict with confidentiality interests or overriding security interests of the operator.

(2) The Federal Office shall be granted access to the sites and business premises, including data processing installations and equipment used for federal communications technology, during the periods when the premises are normally available for the relevant business or operational use, insofar this is necessary to fulfil the purposes laid down in paragraph 1.

(3) In the case of third-party systems with an interface to the federal communications technology, the Federal Office may check the security of the interface only with the consent of the third party. For this purpose, it may, with the consent of the third party, inspect the information required for the performance of the task, in particular technical details, strategies, plans and regulations, as well as documents and data carriers of the operator, and make copies free of charge, including in electronic form.

(4) The Federal Office informs about the outcome of its inspection according to the paragraphs 1 to 3

1. the respective inspected operators;

2. the department's information security officer; and

3. the competent legal and technical supervision.

(5) The Federal Office carries out a factual clarification with the inspected entity before finalising the inspection report. The Federal Office should use the communication to make proposals for improving information security, in particular to remedy the deficiencies identified. Section 4(3) shall apply mutatis mutandis to the communication to bodies outside the operator. The Federal Government may, in consultation with the information security officers of the relevant department, instruct federal administration entities to implement the proposals for improvement within a reasonable period of time.

(6) Excluded from the powers provided for in the paragraphs 1 to 3 are controls on foreign information and -communication technology pursuant to Section 9(2) of the Foreign Service Act, in so far as it is located abroad or is operated for abroad or for users abroad. The provisions for the interfaces of federal communications technology in Germany remain unaffected. Further details on sentence 1 shall be laid down in an administrative agreement between the Federal Ministry of the Interior and Community and the Federal Foreign Office.

(7) The powers according to the paragraphs 1 to 3 do not apply within the scope of the Federal Ministry of Defence to the control of information and communications technology used by the armed forces for their purposes or for the Military Counter-Intelligence Service. Information and communication technology of third parties in particular IT service providers, is not excluded, insofar as they are not operated exclusively for the purposes of the armed forces. Sentences 1 and 2 shall not affect the provisions for the interfaces of federal communications technology. Further details shall be laid down in an administrative agreement between the Federal Ministry of the Interior and Community and the Federal Ministry of Defence.

(8) If, in the course of its inspections, the Federal Office establishes that a breach of the obligations laid down in this Act results in a manifest breach of the protection of personal data within the meaning of Article 4(12) of Regulation (EU) 2016/679, which must be reported in accordance with Article 33 of that Regulation, it shall immediately inform the competent supervisory authorities.

(9) The Federal Office shall inform the Budget Committee of the German Bundestag on the application of this provision every calendar year by 30 June of the year following the reporting year.

§ 8

Protection against malware and threats to federal communications technology

(1) In order to protect federal communications technology against threats, the Federal Office may:

1. use automated processes to gather and evaluate log data generated by operating federal communications technology as necessary to recognise, contain or remedy disruptions to or problems with federal communications technology or attacks on federal communications technology,

2. use automated processes to evaluate the data generated at interfaces of federal communications technology as needed to recognise and protect of malware and other significant threats to federal communications technology.

Unless subsequent paragraphs permit additional uses, the automated evaluation of this data and its subsequent complete and non-recoverable deletion must be carried out without delay. The limitations on use shall not apply to log data which contain neither personal data nor data covered by telecommunications privacy. The federal administration entities are obliged to support the Federal Office in measures pursuant to sentence 1 and to ensure that the Federal Office has access to internal log data pursuant to sentence 1 subparagraph 1 and to interface data pursuant to sentence 1 subparagraph 2. Log data of the federal courts may be gathered only with their approval.

(2) Log data pursuant to paragraph 1 sentence 1 subparagraph 1 may be stored beyond the period required for the automated evaluation pursuant to paragraph 1 sentence 1 subparagraph 1, but for no longer than 18 months, insofar as there are factual indications that, in the event of confirmation of a suspicion pursuant to paragraph 4 sentence 2, this may be necessary to avert threats posed by the malware found or to detect and avert other malware or other significant threats to federal communications technology. Organisational and technical measures shall ensure that the data stored in accordance with this paragraph are evaluated only in an automated manner and that access to data stored for more than three months takes place only if there is actual knowledge that the Federal Government is affected by a malware or any other significant threat to the federal communications technology. The data shall be pseudonymised as far as this is possible with automation. Non-automatic processing shall be permitted only in accordance with the following paragraphs. In so far as it is necessary to restore pseudonymised log data, such data must be ordered by the President of the Federal Office or representation in the Office. A record is to be kept of the decision.

(3) Log data may, prior to their pseudonymisation and storage in accordance with paragraph 2, be processed manually to ensure error-free automated evaluation. If there are indications that the error-free automated evaluation is impeded due to a significant error, the personal reference of log data may be restored to ensure the error-free automated evaluation, provided this is necessary in any particular instance. Paragraph 2, sentences 3 to 6 shall apply accordingly.

(4) Use of personal data beyond the restrictions specified in paragraphs 1 and 2 shall be permitted only when certain facts substantiate suspicion that

1. these data could contain malware;

2. these data could have been transmitted using malware;

3. these data could be related to another significant threat to the federal communications technology, or

4. these data could provide information about malware or any other significant threat to the federal communications technology,

and when the data must be processed in order to substantiate or dispel suspicion. If suspicion is substantiated, the further processing of personal data shall be permitted as necessary

1. to protect agains malware of other significant threats to federal communications technology,

2. to protect against threats arising from the malware found; or

3. to recognise and protect against other malware or threats to federal communications technology.

Malware can be removed or its functioning can be hindered. The necessary technical measures may be taken to eliminate any other significant threat to the federal communications technology. The Federal Office may transmit the data to the federal administration entity concerned, where this is necessary for use in accordance with sentences 1 to 4. Non-automated use of data in accordance with sentences 1 and 2 may be ordered only by a Federal Office employee who is qualified to hold judicial office. The order referred to in sentence 4 shall be subject to the consequent transfer powers in accordance with paragraph 6.

(5) The parties involved in the communication process shall be notified at the latest after the detection and defence of a malware or its effects, or of other significant threats to federal communications technology arising from a malware, if they are known or their identification is possible without disproportionate further investigations and do not conflict with the overriding interests of third parties worthy of protection. Notification shall not be necessary if the person to be notified was not significantly affected and it can be assumed that he/she has no interest in being notified. The Federal Office shall present for inspection those cases in which no notification was made to its data protection official and to another Federal Office employee who is qualified to hold judicial office. If the data protection officer data protection official disagrees with the decision of the Federal Office, the notification shall be made after the fact. The decision not to notify shall be documented. The documentation may be used solely for purposes of data protection monitoring. It shall be destroyed after twelve months. In the cases of paragraphs 6 and 7 notification shall be made by the authorities referred to therein in accordance with the provisions applicable to these authorities. If these provisions do not cover notification requirements, the provisions of the Code of Criminal Procedure shall be applied accordingly.

(6) The Federal Office may transmit the personal data used in accordance with paragraph 4 to the law enforcement authorities to prosecute an offence committed by means of a malware or in the context of another significant threat to the federal communications technology pursuant to Sections 202a, 202b, 303a or 303b of the Criminal Code. Furthermore, it can transmit such data

1. to the federal and Länder police zin order to prevent an immediate threat to public security arising from a malware,

2. to the Federal Office for the Protection of the Constitution to inform it of security-threatening or secret service activities for a foreign power, as well as the Military

Counter-Intelligence Service, where such activities are directed against persons, departments or institutions within the scope of the Federal Ministry of Defence,

3. to the Federal Intelligence Service to inform it on facts revealing an international criminal, terrorist or state attack by means of malware or similar harmful information technology means to the confidentiality, integrity or availability of IT systems in cases of major importance relating to the Federal Republic of Germany.

(7) For others purposes, the Federal Office may transmit such data in accordance with: paragraph 4, sentence 1

1. to the law enforcement authorities for the purpose of prosecuting a serious criminal offence, even in a single instance, especially an offence listed in Section 100a(2) of the Code of Criminal Procedure;

2. to the federal and Länder police to avert a threat to the existence or security of the state, or to the life, limb, or liberty of an individual, or to property of substantial value, the preservation of which is in the public interest;

3. to the federal and Länder offices for the protection of the Constitution and the Military Counter-Intelligence Service, when there are concrete indications of activities within the Federal Republic of Germany directed against the protected interests listed in Section 3(1) of the Federal Constitutional Protection Act or Section 1(1) of the Military Counter-Intelligence Service Act through the use of violence or preparatory acts,

4. to the Federal Intelligence Service, when there are concrete indications of suspicion that someone is planning, committing or having committed offences under Section 3(1)(8) of Article 10 of the Act and this is of foreign and security policy importance for the Federal Republic of Germany,

Transmission in accordance with sentence 1, nos. 1 and 2 shall require prior judicial approval. For the procedure under sentence 1, nos. 1 and 2, the provisions of the Law on proceedings in family matters and matters subject to non-contentious proceedings shall apply accordingly. The court with jurisdiction shall be the local court for the district in which the Federal Office has its headquarters. Transmission in accordance with sentence 1, nos. 3 and 4 is carried out in accordance with the order of the Federal Ministry of the Interior and Community; sections 9 to 16 of Article 10 of the Act shall apply accordingly.

(8) All other evaluation of content beyond that specified in the above paragraphs and all other transmission of personal data to third parties shall be prohibited. As far as possible, technical measures are to ensure that no data relating to the core area of the private sphere are collected. As a result of the measures taken by paragraphs 1 to 4, findings from the core area of private life or data referred to in Article 9(1) of Regulation (EU) 2016/679 may not be used. Information from the core area of the private sphere shall be destroyed immediately. This also applies in cases of doubt. The fact that such information was acquired and destroyed shall be documented. The documentation may be used solely for purposes of data protection monitoring. It shall be destroyed when it is no longer needed for these purposes, but no later than at the end of the calendar year following the year of documentation. If in the framework of paragraphs 5 or 6, the content or circumstances of communication between persons listed in Section 53(1), sentence 1 of the Code of Criminal Procedure is transmitted which is subject to these persons' right to refuse to give evidence, these data may be used as evidence in criminal proceedings only if the crime in question is subject to a custodial sentence of at least five years.

(9) Before gathering and using data, the Federal Office shall have a plan for gathering and using data and shall have this plan ready for inspection by the Federal Commissioner for Data Protection and Freedom of Information. This concept must account for the

special protection requirement of governmental communication. The criteria used in automated processes of evaluation shall be documented. The Federal Commissioner for Data Protection and Freedom of Information shall also communicate the results of his/her checks under Section 16 of the Federal Data Protection Act to the departments responsible.

(10) The Federal Office shall report the following information to the Federal Commissioner for Data Protection and Freedom of Information, each calendar year by 30 June of the reporting year:

1. the number of cases in which data as referred to in paragraph 6 sentence 1, paragraph 6, sentence 2, suparagraph 1 or paragraph 7, subparagraph 1 were transmitted, broken down according to the individual authorisation of transmission;

2. the number of personal evaluations as referred to in paragraph 4, sentence 1where the suspicion has been refuted;

3. the number of cases in which the Federal Office refrained from notifying the persons concerned, as referred to in paragraph 5 sentence 2 or 3.

(11) Each calendar year, the Federal Office shall report to the Committee on Internal Affairs of the German Bundestag by 30 June of the year following the reporting year on its application of this provision.

§ 9

Processing of logging data from federal communications technology

(1) The Federal Office may process logging data generated by the operation of the Federal Government's communications technology to avert risks to the Federal Government's communications technology and its components, including technical infrastructures required for the operation of the Federal Government's communications technology, insofar as this is necessary to detect, limit or eliminate faults, errors or security incidents in the Federal Government's communications technology or attacks on the Federal Government's information technology, and insofar as this does not conflict with confidentiality interests or overriding security interests of the agencies concerned.

(2) The federal administration entities are obliged to support the Federal Office in measures pursuant to paragraph 1 and to ensure that the Federal Office has access to internal logging data pursuant to paragraph 1. For this purpose, they may transmit the corresponding logging data to the Federal Office. Section 8 (1), sentence 5, (2) to (5), (9) and (10) shall apply accordingly. Section 7 Paragraph 7 applies accordingly to the obligation referred to in the sentence 1.

§ 10

Ordering of measures to prevent or remedy security incidents

The Federal Office may, on a case-by-case basis, order federal administrative entities to take measures necessary to prevent or remedy a current security incident. Furthermore, the Federal Office may request the federal administration entities to report within a reasonable period of time on the measures ordered in accordance with sentence 1. The relevant information security officer of the department shall be informed of instructions and requests pursuant to sentences 1 and 2 by the Federal Office. The report shall be submit-

ted to the Federal Office and at the same time to the Information Security Officer of the relevant department. Section 4(3) applies accordingly to reporting.

§ 11

Restoring the security or functioning of information technology systems in exceptional cases

(1) If the security or operability of an information technology system of a federal administration entity or a particularly important entity or important entity is affected, the Federal Office may, at the request of the entity or operator concerned or any other authority responsible for the entity or operator concerned, take the necessary measures to restore the security or functioning of the information technology system concerned. In so far as the Federal Office takes initial measures to limit damage and ensure the emergency operation on the spot, no fees or expenses shall be charged for the activities of the Federal Office. This shall be without prejudice to any costs arising from the use of qualified third parties.

(2) An exceptional case pursuant to paragraph 1 exists in particular, where the attack is of particular technical quality or where the prompt restoration of the security or functioning of the information technology system concerned is of particular public interest.

(3) Dhe Federal Office may, in the case of measures taken in accordance with: paragraph 1 process personal or telecommunications confidential data to the extent necessary and appropriate to restore the security or functioning of the information technology system concerned. The data must be deleted immediately as soon as they are no longer needed to restore the security or functioning of the IT system. If, in cases covered by paragraph 4, the data have been passed on to another authority to fulfil its statutory tasks, the Federal Office may, by way of derogation from sentence 2 continue to process until the support of these authorities is terminated. Use for other purposes is prohibited. Section 8 (8) shall apply accordingly.

(4) The Federal Office may disclose information acquired under this provision only with the consent of the requesting party, unless the information does not allow the identity of the person requesting the information to be identified or the information can, mutatis mutandis, be disclosed in accordance with Section 8(6) and (7). This excludes necessary exchanges of information between the Federal Office and the Federal Office for Civil Protection and Disaster Assistance pursuant to Section 3(7) of the umbrella law on strengthening the physical resilience of critical facilities (KRITIS umbrella law). Access to the files kept in proceedings pursuant to paragraph 1 shall not be granted to third parties.

(5) The Federal Office may, with the consent of the applicant, utilise the assistance of qualified third parties for measures pursuant to paragraph 1 if this is necessary for the timely or complete restoration of the security or functionality of the information technology system concerned. The costs incurred in doing so shall be borne by the applicant. The Federal Office may also refer the applicant to qualified third parties. The Federal Office and third parties authorised by the applicant or by the Federal Office in accordance with sentence 1 may transmit data to each other in the case of measures in accordance with paragraph 1 with the consent of the applicant. Paragraph 3 applies accordingly.

(6) To the extent necessary to restore the security or functioning of the information technology system, the Federal Office may require the manufacturer of the information technology system to contribute to the restoration of security or functioning.

(7) In justified individual cases, the Federal Office may also take action at institutions other than those mentioned in paragraph 1 if the Federal Office has been requested to do

so and if the case is an exceptional case in accordance with paragraph 2. A justified individual case generally exists when a body of a Land is involved.

(8) In the case of facilities or activities which require a permit under the Atomic Energy Act, consultation with the competent nuclear supervisory authorities of the Federation and the Länder shall be established before the Federal Office takes action in the cases referred to in paragraphs 1, 4, 5 and 7. In the case of facilities or activities which require a permit under the Atomic Energy Act, the provisions of the Atomic Energy Act shall take precedence in measures taken by the Federal Office under this Section 11.

§ 12

Inventory data disclosure

(1) The Federal Office may, in order to carry out its statutory task, in accordance with section 3(1), sentence 1, subparagraphs 1, 2, 20, 24 or 25,require information on inventory data pursuant to Section 3(6) of the Telecommunications Act and on the data collected pursuant to Section 172 of the Telecommunications Act (Section 174(1), sentence 1, of the Telecommunications Act) from the person who provides or contributes to the provision of telecommunications services on a commercial basis. The information pursuant to Sentence 1 may only be required in order to protect the supply of the population in the sectors of Section 2, subparagraph 24 or public security, in order to prevent the security or functioning of information technology systems of a particularly important entity or important entity from being compromised, where facts permit the conclusion to be drawn that is at least specific in nature and foreseeable in time and which will target the information technology systems of identifiable infrastructures or undertakings, and where the data to be included in the information are necessary in individual cases in order to enable the persons concerned to comply with oaragraph 4 to warn, inform or advise or assist in the removal of such impairment.

(2) The information under paragraph 1, on the basis of an Internet Protocol address allocated at a given time, may also be requested (Section 174(1), sentence 3, Section 177(1)(3) of the Telecommunications Act). The legal and factual basis of the request for information shall be put on record.

(3) The party obliged to provide information on the basis of a request for information shall provide the data required for the provision of information without delay and in full.

(4) Once the information has been provided, the Federal Office shall inform the particularly important entity or the important entity of the impairments threatening it. As far as possible, the Federal Office shall draw the attention of the particularly important entity or important entity to technical means by which the identified adverse effects can be eliminated by the particularly important entity or important entity itself.

(5) The Federal Office may transmit personal data that it processes under this provision in accordance with Section 8(6) and (7).

(6) In the cases referred to in paragraph 2, the data subject shall be notified of the information. In the case of disclosure of the information pursuant to Section 8(6) or where facts justify the assumption that the conditions for disclosure pursuant to Section 8(6) are met, the data subject will not be notified unless and until there are overriding interests of third parties worthy of protection. If the notification is postponed or dispensed with pursuant to sentence 2, the reasons shall be put on record.

(7) The Federal Office shall inform the Federal Commissioner for Data Protection and Freedom of Information by 30 June of the year following the year under review regarding:

1. the total number of transactions in which data according to paragraph 1 or paragraph 2 were sent to the Federal Office, and

2. the transmissions referred to in paragraph 5.

(8) The Federal Office shall compensate the obligated parties for information provided to it. The amount of compensation shall be determined in accordance with Section 23 and Annex 3 of the Judicial Remuneration and Compensation Act (Justizvergütungs- und -entschädigungsgesetz); the provisions on limitation in Section 2(1) and (4) of the Judicial Remuneration and Compensation Act (Justizvergütungs- und -entschädigungsgesetz) shall apply accordingly.

§ 13

Warnings

(1) In order to perform its tasks under section 3(1) sentence 2 subparagraphs 20 and 21, the Federal Office may

1. address the following warnings and information to the public or interested parties:

   a) warnings of vulnerabilities and other security risks in information technology products and services;

   b) malware warnings,

   c) warnings in the event of loss or unauthorised access to data;

   d) informations on security-related IT properties of products; and

   e) informations on failure to comply with the obligations under this Act by particularly important entities or important entities; and

2. recommend security measures and the use of certain security products.

The Federal Office may involve third parties for the performance of the tasks referred to in sentence 1 if this is necessary for an effective and timely warning.

(2) The manufacturer of affected products shall be informed in good time before the warnings are published. This information obligation does not exist,

1. if this would jeopardise the attainment of the objective pursued by the measure; or

2. if it can reasonably be assumed that the manufacturer has no interest in prior notification.

If identified vulnerabilities or malware are not intended to be made generally known in order to prevent further dissemination or illegal exploitation or because the Federal Office is obliged confidentiality to third parties, it can restrict the circle of individuals to be warned. Criteria for the selection of the circle of individuals to be warned according to sentence 3 are in particular the particular danger of certain facilities or the particular reliability of the recipient.

(3) In order to perform its tasks in accordance with Section 3(1) sentence 2 subparagraphs 20 and 21, the Federal Office may

1. warn the public of vulnerabilities in information technology products and services and of malware, stating the name and manufacturer of the product and service concerned, if there are sufficient indications that they pose a threat to information technology security; or

2. recommend security measures and the use of certain information technology products and services.

If the information provided to the public subsequently proves to be incorrect or if the underlying circumstances turn out to be inaccurate, this shall be made public without delay. Warnings according to sentence 1 shall be removed six months after publication unless there is still sufficient evidence that risks to information technology security exist. If a warning is not removed in accordance with sentence 3, this decision must be reviewed regularly.

§ 14

Security investigation in information technology, request for information

(1) The Federal Office may, in order to carry out its tasks in accordance with: Section 3(1), sentence 2, subparagraphs 1, 20, 21, 24 or 25 investigate information technology products and systems made available on the market or intended to be made available on the market. It may use the support of third parties for this purpose, provided that this does not conflict with the legitimate interests of the manufacturer of the products and systems concerned.

(2) Where necessary, the Federal Office may request all necessary information, in particular technical details, from manufacturers of information technology products and systems for investigations pursuant to paragraph 1 sentence 1. In the request for information, the Federal Office shall state the legal basis, the purpose of the request for information and the information required, and shall set a reasonable time limit for the provision of the information. The request for information shall also contain a reference to the penalties provided for in Section 65.

(3) The Federal Office shall pass on information as well as the findings obtained from the investigations without delay to the competent federal supervisory authorities or, if there is no supervisory authority, to the respective department if there are indications that the supervisory authorities require them in order to fulfil their duties.

(4) The information and findings obtained from investigations may be used only for the purpose of carrying out the tasks referred to in Section 3(1), sentence 2, subparagraphs 1, 20, 21, 24 and 25. The Federal Office may share and publish its findings in so far as this is necessary for the performance of the tasks referred to in Section 3(1), sentence 2, subparagraphs 1, 20, 21, 24 and 25 above. Prior to this, the manufacturer of the products and systems concerned shall be given an opportunity to comment within a reasonable period of time. An opportunity to comment may be waived if the findings are shared or made public with no discernible link to the manufacturer or to the information technology products and systems under investigation.

(5) If a manufacturer does not comply with or only insufficiently complies with the Federal Office's request pursuant to paragraph 2, sentence 1, the Federal Office may inform the public thereof. It may provide the name of the manufacturer, the name of the product or system concerned and indicate the extent to which the manufacturer has failed

to fulfil its obligation to provide information. Prior to this, the manufacturer shall be given an opportunity to comment within a reasonable period of time. Section 13 Paragraph 2, sentence 2 shall apply accordingly.

§ 15

Detection of attack methods and security risks for network and IT security

(1) The Federal Office may, within the scope of its duties under Section 3(1), sentence 2, subparagraphs 1, 2, 20 or 24 carry out queries at the interfaces of publicly accessible information technology systems to public telecommunications networks in order to detect known vulnerabilities and other security risks in federal administrative bodies, at particularly important entities or at important entities;

1. to determine whether these interfaces may be insufficiently protected and thereby jeopardise their safety or functioning; or

2. if requested by the relevant entities.

The information thus obtained may be used only for the purpose of the information referred to in paragraph 2. If the Federal Office obtains information protected by Article 10 of the Basic Law, it must be deleted immediately.

(2) If a known vulnerability or other security risk of an information technology system is recognised through queries in accordance with paragraph 1, the Federal Office shall immediately inform those responsible for the information technology system. If the information technology system is part of a federal administrative entity, the information security officers of the relevant entity of the Federal Administration, in accordance with Section 45 and of the higher-level department in accordance with Section 46 shall be informed at the same time. The Federal Office should draw attention to existing ways of remedying the safety risk. If the parties responsible are not known to the Federal Office or if it is only possible to identify them with disproportionate effort or by means of an inventory data query pursuant to Section 12, the operating service provider of the respective network or system shall alternatively be notified without delay if overriding security interests do not conflict with this.

(3) Tas Federal Office, the Federal Commissioner for Data Protection and Freedom of Information shall inform the Federal Commissioner or the Federal Commissioner for Data Protection and Freedom of Information by 30 June of the following year of the number of queries carried out in accordance with paragraph 1.

(4) The Federal Office shall, upon request, submit to the Federal Commissioner or the Federal Commissioner for Data Protection and Freedom of Information for the purposes of the queries referred to in paragraph 1 a list of the audited systems of the federal administration’s entities, of the particularly important entities and of the important entities for inspection.

(5) In order to fulfil its tasks, the Federal Office may use systems and procedures that make an attacker believe that an attack has been successful in order to survey and evaluate the use of malware or other attack methods. In doing so, the Federal Office may process the data required to evaluate the way the malware and attack methods work.

§ 16

Ordering measures by the Federal Office against telecommunication services providers

(1) In order to prevent significant threats to the protected interests referred to in paragraph 2, the Federal Office may order that a provider of publicly accessible telecommunications services within the meaning of the Telecommunications Act (provider of publicly accessible telecommunications services) with more than 100,000 customers

1. takes measures specified in Section 169(6) and (7) of the Telecommunications Act, or

2. distribute technical commands for cleaning up specifically named malware to affected IT systems;

if and to the extent that the provider of publicly accessible telecommunications services is technically able to do so and it is economically reasonable for him to do so. Prior to the Federal Office ordering the measures pursuant to sentence 1, subparagraphs 1 or 2, an agreement shall be reached with the Federal Network Agency. Prior to the Federal Office ordering the measure pursuant to sentence 1, subparagraph 2, an agreement shall additionally be reached with the Federal Commissioner for Data Protection and Freedom of Information. The data to be accessed using the measure pursuant to sentence 1, subparagraph 2 shall be specified in the order. Section 8 Paragraph 8, sentences 2 to 8 shall apply accordingly. Objections and actions for annulment against the orders pursuant to sentence 1 shall have no suspensive effect.

(2) Protected goods in accordance with paragraph 1, sentence 1 are availability, integrity or confidentiality

1. of the federal communication technology, a particularly important entity or an important entity,

2. information or communications services; or

3. information, insofar as its availability, integrity or confidentiality is restricted by unauthorised access to telecommunications or IT systems of a significant number of users.

(3) If the Federal Office orders a measure in accordance with paragraph 1, sentence 1, subparagraph 1, it may also order the provider of publicly available telecommunications services to redirect traffic to a connection identifier designated by the Federal Office.

(4) The Federal Office may process data that has been redirected by a provider of publicly accessible telecommunications services in accordance with paragraph 1, sentence 1, subparagraph 1, and paragraph 3 in order to obtain information on malware or other security risks in IT systems. The transmitted data may be stored by the Federal Office for as long as is necessary to fulfil the purpose stated in sentence 1, but for no longer than three months. Section 8 Paragraph 8, sentences 2 to 8 shall apply accordingly. The Federal Office shall inform the Federal Commissioner for Data Protection and Freedom of Information by 30 June of the following year of the total number of data diversions ordered.

§ 17

Ordering measures by the Federal Office against digital service providers

The Federal Office may, in individual cases, in order to prevent significant threats to information technology systems of a large number of users who emanate from digital services providers pursuant to Section 2(2)(1) of the Telecommunications-Digital Services Act – Data Protection Act, are insufficiently secured by insufficient technical and organisational measures pursuant to Section 19(4) of the Telecommunications-Digital Services Act and thus do not provide sufficient protection against:

1. unauthorised access to the technical facilities used for those digital services; or

2. disturbances, including if they are caused by external attacks;

order the respective provider of digital services pursuant to Section 2(2)(1) of the Telecommunications-Digital Services Data Protection Act to take the technical and organisational measures necessary to bring its digital services into line with the orderly condition of its digital services. The competence of the supervisory authorities of the federal states shall remain unaffected in all other respects.

§ 18

Ordering measures by the Federal Office against manufacturers of ICT products

Where necessary, the Federal Office may require a manufacturer whose ICT products are affected by significant security incidents to participate in the elimination or avoidance of significant security incidents involving particularly important entities and important entities.

§ 19

Provision of IT security products

The provision of IT security products by the Federal Office in accordance with Section 3(1), sentence 2, subparagraph 15 is carried out by self-development or after a procurement procedure has been carried out on the basis of a corresponding assessment of needs. IT security products can only be provided in justified exceptional cases by an in-house development of the Federal Office. The provisions of public procurement law and the Federal Budget Code remain unaffected. If the Federal Office provides IT security products, the federal administration’s entities or third parties mandated by them can consult them from the Federal Office.

Chapter 2

Data processing

§ 20

Personal data processing

(1) The processing of personal data by the Federal Office is permitted if the processing is necessary for the performance of its tasks in the public interest.

(2) Without prejudice to Article 6(4) of Regulation (EU) 2016/679 as amended and to Section 23 of the Federal Data Protection Act, the processing of personal data by the Federal Office for purposes other than the one for which the data were initially collected is permitted if:

1. the processing is required

   a) to collect, analyse or investigate information on security risks or information technology security measures; or

   b) to provide support, advice or warning on information technology security issues; and

2. there is a reason to assume that the data subject's legitimate interest in the exclusion of processing prevails.

(3) By way of derogation from Article 9(1) of Regulation (EU) 2016/679 and without prejudice to Section 22(1) of the Federal Data Protection Act, the processing of special categories of personal data by the Federal Office shall be permitted if:

1. the processing is necessary for the prevention of a significant threat to network, data or information security;

2. excluding such data from processing would make the performance of the Federal Office's tasks impossible or significantly jeopardise them, and

3. there is a reason to assume that the data subject's legitimate interest in excluding such data from processing prevails.

(4) The Federal Office provides for appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22(2), sentence 2, of the Federal Data Protection Act.

§ 21

Restriction of data subject rights

The following restrictions apply to the rights of the data subject vis-à-vis the Federal Office, in addition to the exceptions laid down in Regulation (EU) 2016/679. To the extent that this Act contains no or lesser restrictions on the rights of the data subject, the restrictions are, moreover, governed by the provisions of the Federal Data Protection Act.

§ 22

Information obligation in the case of collection of personal data

(1) The obligation to provide information pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 shall not apply, in addition to the exceptions referred to in Articles 13(4) and 14(5) of Regulation (EU) 2016/679, where:

1. the provision of information would jeopardise the proper performance of the tasks under the responsibility of the Federal Office; or

2. the provision of information would otherwise jeopardise public security or public order or the safeguarding of network and information security or would otherwise harm the welfare of the Federal Government or a Land;

and therefore the interest of the data subject in the provision of information must be withdrawn.

(2) If the data subject remains informed in accordance with the paragraph 1, the Federal Office shall take appropriate measures to protect the data subject's legitimate interests, including making the information referred to in Article 13(1) and (2) and Article 14(1) and (2) of Regulation (EU) 2016/679 available to the public in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Federal Office shall set out in writing the reasons for not informing the data subject.

§ 23

Right of access by the data subject

(1) The right of access under Article 15(1) and (2) of Regulation (EU) 2016/679 shall not apply if and to the extent that:

1. the provision of information would jeopardise the proper performance of the tasks which are the responsibility of the Federal Office;

2. the information exchange

   a) jeopardise public security or ensure network and information security; or

   b) would cause prejudice to the well-being of the Federal Government or a Land; or

3. the providing information would jeopardise criminal investigations or prosecution of criminal offences

and therefore the data subject's interest in providing information must be withdrawn.

(2) Section 34 Paragraphs 2 to 4 of the Federal Data Protection Act shall apply accordingly.

§ 24

Right to rectification

(1) The right of the data subject shall not be entitled to rectification and completion in accordance with Article 16 of Regulation (EU) 2016/679 if and to the extent that the exer-

cise of the data subject's rights would jeopardise the proper performance of the tasks under the responsibility of the Federal Office and therefore the data subject's interest in the exercise of those rights must be withdrawn.

(2) In the cases of paragraph 1 the data subject shall have the right to attach a reply to the data for the duration of the processing, where this is necessary for fair and transparent processing.

§ 25

Right to erasure

(1) In the case of non-automated processing, the Federal Office shall not be obliged to erase personal data pursuant to Article 17(1) and (2) of Regulation (EU) 2016/679, in addition to the exceptions referred to in Article 17(3), if:

1. deletion is not possible or is only possible with a disproportionate effort due to the particular nature of the storage; and

2. the data subject's interest in erasure is considered to be low.

In that case, the erasure shall be replaced by a restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679. Sentences 1 and 2 shall not apply, if the personal data have been unlawfully processed.

(2) If erasure is only postponed for a possible judicial review of measures pursuant to Section 8(4), the data may only be used for this purpose without the consent of the data subject. They shall be restricted for other purposes in the processing. Section 8 Paragraph 8 remains unaffected.

§ 26

Right to restriction of processing

The Federal Office's obligation to restrict processing pursuant to Article 18(1)(a) of Regulation (EU) 2016/679 shall not apply for the duration of the verification of the accuracy of the personal data if:

1. the processing or further processing is expressly regulated by this Act; or

2. the restriction of processing would jeopardise the prevention of threats to information technology security.

§ 27

Right to object

The right of the data subject to object pursuant to Article 21(1) of Regulation (EU) 2016/679 shall not apply where:

1. the processing is carried out by an overriding public interest which overrides the interests of the data subject; or

2. legal provisions require the Federal Office to process.

In addition, the Federal Office may process the personal data in addition to Article 21(1), sentence 2, of Regulation (EU) 2016/679 until the Federal Office has verified whether there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

Part 3

Security in the information technology of entities

Chapter 1

Scope of application

§ 28

Particularly important and important entities

(1) Particularly important entities are:

1. operators of critical facilities;

2. qualified trust service providers, Top Level Domain name registries or DNS service providers;

3. providers of publicly available telecommunications services or providers of public electronic communications networks, which:

   a) employ at least 50 employees, or

   b) have an annual turnover and an annual balance sheet total of more than EUR 10 million each,

4. other natural or legal persons or legally dependent organisational units of a local authority that offers goods or services to other natural or legal persons in return for payment, which are assigned to one of the types of facilities specified in Annexe 1 and which:

   a) employ at least 250 employees, or

   b) have an annual turnover of more than EUR 50 million and an annual balance sheet total of more than EUR 43 million.

This exclude federal administrative entities, unless they are also operators of critical facilities.

(2) Important entities are:

1. trust service providers,

2. providers of publicly available telecommunications services or providers of public electronic communications networks, which:

a) employ less than 50 employees; and

b) have an annual turnover and an annual balance sheet total of EUR 10 million or less,

3. natural or legal persons or legally dependent organisational units of a local authority that offers goods or services to other natural or legal persons in return for payment, which are assigned to one of the types of facilities specified in Annexes 1 and 2 and which:

a) employ at least 50 employees, or

b) have an annual turnover and an annual balance sheet total of more than EUR 10 million each.

This exclude particularly important entities and entities of the federal administration.

(3) When determining the number of employees, annual turnover and annual balance sheet total referred to in paragraphs 1 and 2,

1. the business activity attributable to the type of entity shall be taken into account; and

2. except for legally dependent organisational units of a local authority, the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20 May 2003, p. 36), with the exception of Article 3(4) of the Annex, shall apply.

The data of partner or linked enterprises as defined in Recommendation 2003/361/EC shall not be added if the enterprise is independent from its partner or linked enterprises, having regard to the legal, economic and factual circumstances as regards the nature and operation of the information technology systems, components and processes.

(4) The Sections 30, 31, 32, 35, 36, 38, 39, 61 and 62 shall not apply to particularly important entities and important entities which:

1. operate a public telecommunications network or provide publicly available telecommunications services;

2. operate energy supply networks or energy installations as defined in Energy Industry Act of 7 July 2005 (Federal Law Gazette (BGBl.) I p. 1970, 3621), as last amended by Article 1 of the Act of 14 May 2024 (Federal Law Gazette (BGBl.) 2024 I) No 161) and are subject to the provisions of Section 5c of the Energy Industry Act.

Sentence 1 shall not apply to the particularly important and important entities listed therein insofar as they operate further critical facilities in accordance with Section 2 subparagraph 22 in addition to the facilities listed in the first sentence, numbers 1 and 2or are assigned to one of the types of entities specified in Annex 1 or 2 due to further activities. Sentence 2 shall apply to all information technology systems necessary for the operation of the other critical facilities.

(5) The Sections 30, 31, 32, 35, 36, 38 and 39 do not apply to:

1. financial undertakings in accordance with Article 2(2) of Regulation (EU) 2022/2554 and undertakings for which the requirements of Regulation (EU) 2022/2554 on the basis of Section 1a(2) of the Banking Act or Section 293(5) of the Insurance Supervision Act apply,

2. the Telematics Company pursuant to Section 306(1) sentence 3 of the Fifth Book of the Social Security Code, operators of telematics infrastructure services with regard to the services authorised under Section 311(6) and Section 325 of the Fifth Book of the Social Security Code and operators of services insofar as they use the telematics infrastructure for applications confirmed pursuant to Section 327(2) to (5) of Book V of the Fifth Book of the Social Security Code.

(6) Section 32 does not apply to operators of critical facilities insofar as they operate a facility for companies under paragraph 5, subparagraph 1.

(7) A critical facility operator is a natural or legal person or a legally dependent organisational unit of a local authority which, having regard to the legal, economic and factual circumstances, exercises decisive influence over one or more critical facilities. By way of derogation from sentence 1, in the financial sector the person exercising actual control over an investment has decisive influence over it. In that regard, the legal and economic circumstances are not taken into account.

(8) This Act shall not apply to legally dependent organisational units of territorial authorities and to legal entities in which only territorial authorities, with the exception of the Federal Government, are involved, if they:

1. were established for the purpose of providing services to administrations with a public-service mission; and

2. are regulated by comparable provisions of Land law by reference to this paragraph.

§ 29

Entities of the federal administration

(1) Entities of the federal administration within the meaning of this Act, with the exception of social security institutions and the Bundesbank, are:

1. federal authorities;

2. IT service providers of the federal administration organised under public law; and

3. other bodies, establishments and foundations under public law and their associations, irrespective of their legal form, at federal level, if ordered by the Federal Office in agreement with the relevant department.

(2) For entities of the federal administration, the rules for particularly important entities are to be applied, but not the provisions of Sections 38, 40(3) and Sections 61 and 65. In addition, for entities of the federal administration, with the exception of the Federal Chancellery and the federal ministries, the rules of the § 30 are not to be applied.

(3) The business divisions of the Federal Foreign Office and the Federal Ministry of Defence, as well as the Federal Intelligence Service and the Federal Office for the Protection of the Constitution are, in addition to the rules laid down in paragraph 2, sentence 2, excluded from the provisions of the Section 7(5) sentence 4, Section 10, Section 13(1)(1)(e) and of Sections 30, 33 and 35. The Foreign Office, in agreement with the Federal Ministry of the Interior and Community, issues a general administrative regulation in order to implement the objectives of the NIS 2 Directive in the area of activity of the Federal Foreign Office by means of results equivalent measures.

Chapter 2

Risk management, reporting, registration, verification and notification obligations

§ 30

Risk management measures for particularly important entities and important entities

(1) Particularly important entities and important entities shall be required to take appropriate, proportionate and effective technical and organisational measures, specified in accordance with paragraph 2, to avoid disruptions to the availability, integrity and confidentiality of the information technology systems, components and processes they use for the provision of their services and to minimise the impact of incidents. When assessing the proportionality of the measures referred to in sentence 1, account shall be taken of the extent of the risk exposure, the size of the entity, the compliance costs and the likelihood and severity of incidents, as well as their societal and economic impact. Compliance with the obligation under sentence 1 shall be documented by the entity.

(2) Measures taken pursuant paragraph 1 shall respect the state of the art, take into account relevant European and international standards and shall be based on an all-hazard approach. The measures shall include at least the following:

1. concepts on risk evaluation and information technology security;

2. the management of security incidents;

3. business continuity, such as backup management and post-emergency recovery, and crisis management;

4. the integrity of the supply chain, including security-related aspects of the relationship between each entity and its immediate suppliers or service providers;

5. security measures in the acquisition, development and maintenance of information technology systems, components and processes, including vulnerability management and disclosure;

6. concepts and procedures for assessing the effectiveness of information technology security risk management measures;

7. basic procedures in the field of cyber hygiene and training in the area of information technology security;

8. concepts and procedures for the use of cryptography and encryption;

9. staff security, access control and facility management concepts;

10. the use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communication and, where appropriate, secured emergency communication systems within the entity.

(3) The implementing act adopted by the European Commission pursuant to the first subparagraph of Article 21(5) of the NIS 2 Directive laying down the technical and methodological requirements for the measures referred to in paragraph 1 relating to DNS

service providers, top level domain name registries, cloud computing service providers, data centre service providers, content delivery network operators, managed service providers, managed security service providers, providers of online marketplaces, online search engines and social networking platforms and trust service providers shall be prioritised for the aforementioned types of entities.

(4) Provided that the European Commission adopts an implementing act in accordance with Article 21(5)(2) of the NIS 2 Directive, in which the technical and methodological requirements and, where necessary, the sectoral requirements of the measures referred to in Paragraph 2, those requirements shall take precedence over the measures referred to in paragraph 2 to the extent that they conflict with them.

(5) Unless the implementing acts of the European Commission pursuant to Article 21(5) of the NIS 2 Directive contain conclusive provisions on the technical and methodological requirements and, if necessary, on the sectoral requirements for the measures referred to in paragraph 2 with regard to particularly important entities and important entities, these provisions may be specified and extended by the Federal Ministry of the Interior and Community in consultation with the departments concerned by statutory ordinance, which shall not require the approval of the Bundesrat, taking into account the possible consequences of inadequate measures and the importance of certain entities.

(6) Particularly important entities and important entities may, by means of a statutory ordinance, pursuant to Section 56(3) use certainICT products, ICT services and ICT processes only if they have a cybersecurity certification in accordance with European schemes referred to in Article 49 of Regulation (EU) 2019/881.

(7) Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, the exchange of information under Section 6 or voluntary reporting under Section 5 shall not result in the imposition of additional obligations on the reporting entity that would not have applied to it if it had not submitted the report.

(8) Particularly important entities and their industry associations may propose industry-specific safety standards to ensure compliance with the requirements set out in paragraph 1. These proposed safety standards must take into account implementing acts adopted by the European Commission in such a way that they do not conflict with the requirements set out therein and do not fall short of what they contain. Upon request, the Federal Office shall determine whether the proposed safety standards are sector-specific and suitable for guaranteeing the requirements set out in paragraph 1. The determination shall be made

1. In agreement with the Federal Office for Civil Protection and Disaster Assistance;

2. in agreement with the competent supervisory authority of the Federal Government.

In the healthcare sector, if no competent federal supervisory authority exists, consultation with the Federal Ministry of Health shall be established in deviation from sentence 4 subparagraph 2.

(9) Operators of critical facilities may propose sector-specific safety standards to ensure compliance with the requirements under Section 39(1).Paragraph 8 sentences 2 to 5 apply accordingly.

§ 31

Special requirements for the risk management measures of operators of critical facilities

(1) Ffor operators measures in accordance with Section 30(1) sentence 1 that go beyond the level of protection of the information technology systems, components and processes that are decisive for the functionality of the critical facility operated by them shall also be deemed proportionate in comparison to other information technology systems, components and processes of particularly important entities if the effort required for this is not disproportionate to the consequences of a failure or impairment of the critical facility concerned.

(2) Operators of critical facilities are obliged to use systems to detect attacks. The systems used for detecting attacks must continuously and automatically record and evaluate suitable parameters and features from ongoing operations. They should be able to identify and prevent threats on an ongoing basis and provide for appropriate remedial actions for incidents that have occurred. The state of the art shall be observed. The effort required for this purpose should not be disproportionate to the consequences of a failure or impairment of the critical facility concerned.

§ 32

Reporting obligations

(1) Particularly important entities and important entities are obliged to report the following information to a joint reporting unit set up by the Federal Office and the Federal Office for Civil Protection and Disaster Assistance:

1. without delay and at the latest within 24 hours of becoming aware of a significant incident in an early initial notification indicating whether there is a suspicion that the significant incident is due to an illegal or malicious act or may have a cross-border impact;

2. without delay and at the latest within 72 hours of becoming aware of a significant incident a significant incident notification confirming or updating the information referred to in subparagraph 1 and indicating an initial assessment of the significant incident, including its severity and impact, and, where applicable, the compromise indicators;

3. auf request of the Federal Office, an interim report of relevant status updates;

4. no later than one month after the submission of the security incident report referred to in subparagraph 2, subject to paragraph 2, a final report containing the following:

   a) a detailed description of the incident, including its severity and impact;

   b) information on the nature of the threat or underlying cause that is likely to have triggered the incident;

   c) information on the corrective measures taken and ongoing;

   d) where applicable, the cross-border impact of the incident.

   The obligation referred to in the sentence 1 shall apply at the earliest from the establishment of the reporting channel.

(2) If the security incident is still ongoing at the time referred to in paragraph 1(4), the organisation concerned shall submit a progress report instead of a final report at that time. The final report must be submitted to the Federal Office after the security incident has been completed by the entity concerned.

(3) Operators of critical facilities shall also be required to provide information on the nature of facility and critical service affected and the impact of the security incident on that service if a significant security incident has or could have an impact on the critical facility they operate.

(4) The Federal Office, in agreement with the Federal Office for Civil Protection and Disaster Assistance, shall lay down the details of the form of the reporting procedure and the details of the report content, after consulting the operators concerned and the business associations concerned, provided that they do not conflict with possible implementing acts of the European Commission. The information referred to in sentence 1 shall be published by the Federal Office on its website.

(5) The Federal Office shall make the reports it receives available to the competent federal supervisory authorities without delay.

(6) The Federal Office may reporting entities in accordance with the Section 36(1) Offer their assistance in resolving the incident.

§ 33

Registration obligation

(1) Particularly important and important entities as well as domain name registry service providers shall be required to submit the following information to the Federal Office through a registration entity established jointly by the Federal Office and the Federal Office for Civil Protection and Disaster Assistance no later than three months after they are considered to be one of the above-mentioned entities or provide domain name registry services:

1. Name of the entity, including the legal form and, where applicable, the trade register number

2. Address and up-to-date contact details, including e-mail address, public IP address and telephone numbers;

3. the sector referred to in Appendix 1 or 2 or, where applicable, sector;elevanter in

4. member States of the European Union in which the facility provides services of the types of facilities listed in Appendix 1 or 2; andlist of those

5. The competent federal and Länder supervisory authorities for the activities on the basis of which registration is carried out.

(2) Operators of critical installations shall submit, with the information referred to in paragraph 1, the critical service, the public IP address areas of the installations they operate, as well as the category of installations identified for the critical installations they operate and the supply ratios determined in accordance with the statutory ordinance pursuant to: Section 56(4) and the location of the installations and a contact point. ensure that they can be contacted at all times through their contact point referred to in the first sentence. The operators:

(3) Doha Federal Office may, in agreement with the relevant competent supervisory authorities, carry out its own registration of key entities and important entities and domain name registration service providers if their registration obligation is not fulfilled.

(4) that an entity is required to register in accordance with: authentic facts the adoptionParagraph 1 or 2 this institution shall, on request, submit to the Federal Office the records, documents and other documents required by the Federal Office for the Assessment in an appropriate manner and provide information, unless security interests or overriding security interests conflict.

(5) In the event of amendments in accordance with Paragraph 1 or 2, changed care figures must be transmitted to the Federal Office once a year and all other information must be transmitted immediately, but no later than two weeks from the date on which the institution became aware of the change.

(6) The Federal Office shall lay down the detailed arrangements for the registration procedure in agreement with the Federal Office for Civil Protection and Disaster Assistance. The determination pursuant to sentence 1 shall be made by means of a public communication on the website of the Federal Office.

§ 34

Specific registration obligation for certain types of entities

(1) An-institution which is to be found in Section 60(1), first sentence the following information shall be provided to the Federal Office no later than three months after it is considered to be one of the above-mentioned establishments:

1. NAME of the institution;

2. einconvenient sector, industry and type of institution as in Appendix 1 determined;

3. Aletter of principal place of business in the European Union in accordance with: Section 60(2) and ihany other establishment in the European Union or, if not established in the European Union, his address to: Section 60(3) appointed representatives;

4. aup-to-date contact details, including e-mail addresses and telephone numbers of the institution and, where necessary, its following Section 60(3) appointed representatives;

5. The Member States of the European Union in which the entity provides services; and

6. The public IP—Addres areas of the institution.

(2) In case of an amendment to the provisions of Paragraph 1, information provided shall inform the institutions of the Section 60(1), first sentence the type of establishment referred to the Federal Office immediately following that change, but at the latest within three months of the date on which the change occurred.

(3) With the exception of the information specified inParagraph 1, point 6, the Federal Office shall forward the information referred to above: Section 34 forward information to the European Union Agency for Cybersecurity.

(4) DAS Bundesamt may, for the purposes of transmitting the information in accordance with the Paragraphs 1 and 2 provide for an appropriate reporting channel.

§ 35

Directional obligations

(1) In the event of a significant incident, the Federal Office may order particularly important entities and entities to immediately inform the recipients of its services of that significant incident, which could affect the provision of the service concerned. The Federal Office shall inform the federal supervisory authority responsible for the establishment of the instructions referred to in the first sentence. The information referred to in the first sentence may also be provided by publication on the institution's website.

(2) Edirections to Paragraph 1, first sentence from the sectors of finance, social security institutions and basic income for job seekers, digital infrastructure, ICT services management and digital services, shall immediately notify the recipients of their services potentially affected by a significant cyber threat and the Federal Office of any measures or remedies that those recipients may take in response to that threat. At the same time, the entities shall also inform those recipients of the significant cyber threat themselves. The obligations under the first or second sentence shall apply only if the interests of the entity and the beneficiary outweigh the interests of the recipient.

§ 36

Feedback from the Federal Office vis-à-vis reporting entities

(1) In the event of a notification from an entity in accordance with: Section 32 the Federal Office shall, without undue delay and where possible within 24 hours, send it a confirmation of receipt of the notification and, at the request of the institution, guidance or operational advice on remedial action. The Federal Office may provide additional technical assistance at the request of the body concerned.

(2) If a faising If raising public awareness is necessary to prevent or manage a significant security incident, or if disclosure of the significant security incident is otherwise in the public interest, the Federal Office may, after hearing the organisation concerned, require it to inform the public about the significant security incident. The Federal Office may also inform the public itself in accordance with the conditions laid down in the first sentence. If the body concerned is a federal administrative body, information to the public shall apply: Section 4(3) correspondingly.

§ 37

Notice of acceptance

(1) Das the Federal Ministry of the Interior and Community may, on a proposal from the Federal Chancellery, the Federal Ministry of Justice, the Federal Ministry of Defence, the Federal Ministry of Finance, the Ministries of the Interior and Justice of the Länder or on its own initiative, a particularly important body or obligations under this Act in accordance with the Paragraph 2 partially exempt (simple exemption decision) or in accordance with the Paragraph 3 exempt in total (extended exemption decision), provided that the institution complies with requirements equivalent to the obligations under this Act. The decision referred to in the first sentence shall be taken with the relevant ministry in agreement and, in the case of the Ministries of the Interior and Justice of the Länder, in consultation.

(2) Facilities; the

1. O perate (relevant areas) or provide services in the fields of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences; or

2. finally, for Public authorities performing tasks in relevant areas, operating or providing services;

may, for those activities or services, be subject to risk management measures in accordance with: Section 30 and the reporting obligations under: Section 32 be exempted. in such cases, the information technology of these facilities must be ensured and supervised by other means. Security

(3) Entities, which operate or provide services exclusively in relevant areas may be wholly exempted from the obligations set out in paragraph (2) and from the registration obligations under Section 33 and Section 34. Paragraph 2, sentence 2 shall apply accordingly.

(4) Paragraphs 1 to 3 shall not apply where the entity concerned is a trust service provider.

(5) An exemption decision under that law shall be revoked if facts subsequently arise that should have led to the refusal to grant an exemption. By way of derogation from: Sentence 1 in the event of temporary cessation of the conditions laid down in the Paragraph 2, point 1 or 2 refrain from revocation.

§ 38

Implementation, monitoring and training obligation for management of particularly important institutions and important institutions

(1) Management of particularly important entities and important entities shall be required to be carried out by such entities in accordance with: Section 30 implement risk management measures to be taken and monitor their implementation.

(2) Gemployees who fail to comply with their obligations under paragraph 1 shall be liable for any culpable damage caused to their body in accordance with the rules of company law applicable to the legal form of the entity. Under that Act, they are liable only if the company law provisions governing the entity do not contain any liability regime under sentence 1.

(3) The business management particularly important institutions and institutions shall undergo regular training in order to acquire sufficient knowledge and skills to identify and assess risks and risk management practices in the area of information technology security and to assess the impact of risks and risk management practices on the services provided by the institution.

§ 39

Non-compliance obligations for Operators of critical installations

(1) Operators of critical installations must implement the measures in accordance with: Section 30(1), first sentence in connection with Section 31(1) and (2), first sentence at a date determined by the Federal Office in consultation with the Federal Office for Civil Protection and Disaster Assistance, at the earliest three years after the first time, or at the latest three years after they are considered a critical installation operator, and every three

years thereafter to the Federal Office by means of security audits, audits or certifications. Operators shall submit to the Federal Office the results of the audits, audits or certifications carried out, including information on the safety deficiencies identified. The Federal Office may request the submission of the documentation on which the verification was based. In the case of safety deficiencies, it may require the submission of an appropriate plan of remedial measures and, in agreement with the competent federal supervisory authority or in consultation with the other competent supervisory authority, that the safety deficiencies be remedied. The Federal Office may require the submission of appropriate proof of the remedial action taken.

(2) The Federal Office may lay down the following requirements for the organisation of the procedure for testing and the provision of evidence referred to in paragraph 1:

1. An claims on the manner in which they are to be implemented;

2. Arequests for the appropriateness of the evidence to be provided, and

3. Nconsultation of the operators and institutions concerned and the business associations concerned, technical and organisational requirements for the auditing bodies in agreement with the Federal Office for Civil Protection and Disaster Assistance.

The determination referred to in the first sentence shall be made by means of a public communication on the website of the Federal Office.

(3) Aby way of derogation from the first sentence of paragraph 1, the Federal Office for Operators of Critical Installations which, until the entry into force of this Act, were critical infrastructure operators pursuant to Section 2(10) of the BSI Act of 14 August 2009 (BGBl. I, p. 2821), as last amended by Article 12 of the Act of 23 June 2021 (BGBl. I, p. 1982), the date of submission of evidence not earlier than three years after the last proof referred to in Section 8a(3) of the BSI Act of 14 August 2009 (BGBl. I, p. 2821), as last amended by Article 12 of the Act of 23 June 2021 (BGBl. I, p. 1982), fixed.

§ 40

National liaison office and central reporting— and contact point for particularly important and important entities

(1) The Federal Office is the national liaison office as well as the single reporting and supervisory contact point for particularly important entities and information technology security entities.

(2) To fulfil its role as national liaison office, the Federal Office coordinates

1. The cross-border cooperation between the Länder authorities that the Länder have designated as competent authorities for the supervision of public administration entities at regional level pursuant to Article 2(2)(f)(ii) of the NIS 2 Directive, as well as the Federal Agency for Financial Services Supervision, with the competent authorities of other Member States responsible for monitoring the application of the NIS 2 Directive and, where appropriate, with the European Commission and the European Union Agency for Cybersecurity;

2. Such as the cross-sectoral cooperation Point 1 the federal state authorities, the Federal Office for Civil Protection and Disaster Assistance, the Federal Network Agency and the Federal Institute for Financial Services Supervision.

(3) Tots task as a central reporting office, the Federal Office must

1. collect collect and analyse information essential for the prevention of threats to information technology security, in particular information on vulnerabilities, malware and attacks,

2. The Relevance of the analyse of this information in accordance with point 1 for the availability of critical services in cooperation with the competent supervisory authorities and the Federal Office for Civil Protection and Disaster Assistance;

3. the situational picture information technology security of critical facilities; particularly important and important institutions continuously update and

4. Immediatelymmediately inform

   a) the operatorsof critical installations about information relating to them according to the points 1 to 3 of Section 33(1)(2)

   b) the competent authorities of another Member State of the European Union on Paragraph 5 inform significant disruptions that have an impact in that Member State, as notified under similar arrangements, taking into account the interests of national security and defence; and

   c) Das Foreign Office on Section 32(1) notify notified significant international security incidents; and

   d) within the framework of processes agreed in advance between the Federal Office and the recipients for forwarding and maintaining the necessary confidentiality, to inform the authorities designated by the Länder as central contact points for this purpose or the competent federal authorities of the information required to fulfil their tasks.

   (4) Zthe Federal Office is responsible for carrying out its duties as one-stop shop

1. questions raised in Paragraph 2 adopt and send them to the competent authorities in Paragraph 2 forward to the designated bodies,

2. R refer to the Paragraph 2, point 2 create such requests with the involvement of the bodies referred to in paragraph 1 or replies from: Paragraph 2 the addresses indicated in: Paragraph 2 forward to the designated bodies to: Section 32 forward notifications received to the single points of contact of the other Member States of the European Union concerned;

3. where a significant incident involves two or more Member States of the European Union, inform the other Member States concerned and the European Union Agency for Cybersecurity of the significant incident, specifying the type of: Section 32(2) to communicate information received and to safeguard the economic interest of the entity and the confidentiality of the information provided.

(5) During a significant incident in accordance with Section 32(1) the Federal Office may, in agreement with the relevant competent federal supervisory authority, require the operators of critical installations concerned to provide the information, including personal data, necessary to deal with the disruption. Operators of critical installations shall be authorised, upon request, to provide the Federal Office with the information necessary to deal with the incident, including personal data, to the extent necessary to deal with a significant incident.

(6) In the context of this provision, processing of personal data beyond the previous paragraphs is prohibited for other purposes. Section 8 Paragraph 8, sentences 3 to 9 apply mutatis mutandis.

§ 41

Prohibition of the use of critical components

(1) Operators of critical installations have the planned initial deployment of a critical component in accordance with: Section 2(23) notify the Federal Ministry of the Interior and Community prior to their deployment. The notification shall specify the critical component and the planned nature of its use. Sentence 1 does not apply to an operator of critical installations if it already deploys another critical component of the same type for the same type of deployment in accordance with: Sentence 1 has been notified and has not been prohibited from operating.

(2) The Federal Ministry the intended initial deployment of a critical component vis-à-vis the operator of critical installations in consultation with the: Section 56(4) crownif the intervention is likely to affect the public policy or public security of the Federal Republic of Germany, the relevant departments and the Federal Foreign Office prohibited or issued orders until two months from the date of receipt of the notification referred to in paragraph 1. At the In particular, consideration may be given to the assessment of likely prejudice to public policy or public security whether:

1. the manufacturer is controlled, directly or indirectly, by the government of a third country, including any other public bodies or armed forces;

2. the manufacturer has already been or is involved in activities that have had an adverse effect on the public policy or security of the Federal Republic of Germany or of any other Member State of the European Union, the European Free Trade Association or the North Atlantic Treaty, or on its facilities; or

3. the use of the critical component is in line with the security policy objectives of the Federal Republic of Germany, the European Union or the North Atlantic Treaty.

Use shall not be permitted before the expiry of the period of two months following the notification referred to in paragraph 1. The Federal Ministry of the Interior and Community may extend the time limit to the institution by a further two months if the examination reveals particular difficulties of a factual or legal nature.

(3) Critical components according to Section 2(23)shall only be used if the manufacturer has made a declaration of trustworthiness (guarantee statement) to the operator of the critical installation. shall be attached to the notification referred to in paragraph 1. The guarantee statement The guarantee shall state how the manufacturer can ensure that the critical component does not have any technical properties that are specifically capable of exerting an abusive influence on the security, integrity, availability or functionality of the critical infrastructure, in particular for the purpose of sabotage, espionage or terrorism. The Federal Ministry of the Interior and Community shall set out the details of the minimum requirements for the guarantee statement in agreement with the Section 56(4) crownidentified the relevant departments and the Federal Foreign Office by means of a general order, which must be published in the Federal Gazette. The details of the minimum requirements for the guarantee statement shall be based on the protection objectives of security, confidentiality, integrityfollow the availability and functioning of the critical facility and the prevention of threats to public order and security, in particular: Paragraph 2, second sentence‘addressing from the sphere of the manufacturer of the critical component, in particular its organisational structure. The first and second sentences shall apply only from the date of publication of the general order referred to in the fourth sentence and not for critical components already used before that date. Insofar as amendments are made to the general decree, these shall be irrelevant to guarantees already issued pursuant to this paragraph.

(4) The Federal Ministry of the Interior and Community may continue to deploy a critical component vis-à-vis the operator of critical installations in agreement with the following: Section 56(4) crownprohibited or ordered the relevant departments and the Foreign Office if further deployment is likely to affect the public order or security of the Federal Republic of Germany, in particular if the manufacturer of the critical component is not trustworthy. Paragraph 2, second sentence paragraph 5.1(i) will apply mutatis mutandis.

(5) A manufacturer of a critical component is deemed not to be trustworthy, in particular where there is sufficient evidence that:

1. eR has failed to fulfil the obligations entered into in the guarantee statement;

2. Ithe factual allegations made in the guarantee statement are false;

3. it does not adequately support safety checks and penetration analyses to the required extent in its product and in the production environment;

4. Sdoes not remove any watching or tampering with its product immediately upon becoming aware of it and notify the operator of critical installations;

5. Dthe critical component has, due to defects, an increased risk potential or has shown abuse to influence the security, confidentiality, integrity, availability or functionality of the critical asset; or

6. The critical component has or has had technical characteristics that are or have been specifically capable of affecting the security, confidentiality, integrity, availability or functionality of the critical asset.

(6) According to paragraph 4 prohibiting the continued use of a critical component, the Federal Ministry of the Interior and Community may, in agreement with the Section 56(4) the respective departments concerned and the Federal Foreign Office

1. Dprohibit the planned use of other critical components of the same type and manufacturer; and

2. prohibit the use of critical components of the same type and from the same manufacturer that are already in use, after a reasonable period of time.

(7) Where there is no trustworthiness under paragraph 5, the Federal Ministry of the Interior and Community may use all the critical components of the manufacturer in agreement with the Section 56(4) prohibit the departments concerned and the Federal Foreign Office.

§ 42

Request for information

Access to information and files on matters covered by Part 2 Sections 4 to 10 and Part 3 this Act shall not be granted. The rights of access to the file of parties to the proceedings shall remain unaffected.

Chapter 3

Information security of federal administrative bodies

§ 43

Information security management

(1) The management of the establishment of the Federal Administration is responsible for creating the conditions for ensuring information security, taking into account the needs of IT operations.schaffen.

(2) The management of the establishment of the federal administration must undergo regular training in order to acquire sufficient knowledge and skills to identify and assess risks and risk management practices in the area of information security and to assess the impact of risks and risk management practices on the services provided by the institution.

(3) Swhere bodies organised under public or private law are entrusted with the provision of information technology services by the Federal Government, contractually ensure that they undertake to comply with the conditions for ensuring information security. This also applies in the event that interfaces with the communication technology of the Federal Government are set up. This shall be without prejudice to the duties of the management of the establishment of the federal administration under paragraph 1.

(4) The registration from federal administration bodies to Section 33 is responsible for the management of the establishment of the federal administration. The Federal Administration shall demonstrate to the Federal Office that the requirements have been met. The institutions shall:Paragraph 1 No later than five years after the entry into force of this Act and regularly thereafter in accordance with its requirements.

(5) When, the reporting obligations of Section 32 are made public, the institutions of the federal administration information in accordance with Section 4(2), point 1which are relevant for the performance of tasks or for the security of the federal communications technology shall inform the Federal Office of this without delay, unless otherwise required. the reporting obligations for federal administrative bodies in accordance with: Except for:Section 32 and to Sentence 1 this paragraph is information which may not be disclosed on the basis of rules on security of information or agreements with third parties, or whose disclosure would be contrary to the constitutional status of a Member of the Bundestag or a constitutional body or to the independence of individual bodies laid down by law. The federal administration institutions shall report to the Federal Office by 31 January each year the total number of Second sentence non-submitted information. The Federal Intelligence Service and the Federal Office for the Protection of the Constitution shall be exempt from the obligation under the third sentence of paragraph 5.

(6) TDhe Federal Ministry of the Interior and Community shall, in agreement with the departments concerned, adopt general administrative provisions for the implementation of the Paragraph 5.

§ 44

Specifications of the Federal Office

(1) The federal administration institutions must comply with the current versions of the minimum standards for security in Federal Information Technology (minimum standards) as minimum requirements for the protection of information processed in the federal administration. The minimum standards shall be: Federal Office determined in consultation with the departments and other supreme federal authorities and published on the website of the Federal Office. Deviations from the minimum standards are only permitted in objectively justified cases and must be documented and substantiated. For the Section 2, point 21 the provisions referred to in the first sentence shall be recommended by the courts and constitutional bodies referred to in the first sentence. The exceptions provided for in the first sentence shall apply to the obligation referred to in the first sentence: Section 7(6) and (7) correspondingly.

(2) The Federal Chancellery and the Federal Ministries must comply with the BSI standards and the IT-Grundschutz Compendium of the Federal Office (IT-Grundschutz) as additional minimum requirements, as amended. The versions in force are published on the website of the Federal Office. Basic IT protection is regularly evaluated by the Federal Office and in accordance with the state of the art and in the light of the experience gained from practice and advice and support in accordance with: Paragraph 4 further developed; the implementation burden is minimised as far as possible. The Federal Office will modernise and develop basic IT protection by 1 January 2026. The exceptions provided for in the first sentence shall apply to the obligation referred to in the first sentence: Section 7(6) and (7) correspondingly.

(3) Das a result of the implementation of the minimum requirements referred to in the first sentence of paragraph 1, and Paragraph 2, first sentenceis compliance with the requirements set out in Section 30 unless the European Commission adopts an implementing act pursuant to the second subparagraph of Article 21(5) of the NIS 2 Directive, in which the technical and methodological requirements go beyond the minimum requirements set out in the first sentence of paragraph 1 and the first sentence of paragraph 2 of this Article. If a federal entity is at the same time an operator of critical installations and the requirements of IT baseline protection and minimum standards are in accordance with: Section 30(9) and Section 31 the latter shall prevail.

(4) The Federal Office advise the federal administration’s institutions, upon request, on how to implement and comply with the minimum requirements under the first sentence of paragraph 1 and the first sentence of paragraph 2, provide tools and support the provision of corresponding solutions by the Federal IT service providers throughout the life cycle.

(5) The Federal Office shall, within the scope of its tasks: pursuant to Section 3(1), second sentence, point 10 technical guidelines and reference architectures which are taken into account by the federal administration bodies as a framework for the development of appropriate requirements for contractors – in the sense of suitability – and IT products – in the sense of a specification – for the conduct of procurement procedures. The provisions of public procurement law and security shall remain unaffected.

(6) With regard to the institutions of the federal administration, the Federal Ministry of the Interior and Community may, in agreement with the other departments, stipulate that they are obliged to comply with: Section 19 retrieve provided IT security products from the Federal Office. In this case, in-house purchases by the federal administration’s facilities are only permitted if the specific profile requires the use of different products. This does not apply to: in Section 2, point 21 citednational courts and constitutional bodies and foreign information and -communication technology in accordance with Section 7(6).

§ 45

Information Security Officers of the Institutions of the Federal Administration

(1) Each head of a federal administration body appoints a body for its institution Information Security Officers or Information Security Officers it shall designate at least one person authorised to represent him or her.

(2) In order to carry out their tasks, the ability of the Information Security Officers necessary for the institutions of the federal administration. The Information security officers the institutions and their representatives must acquire the expertise necessary for the performance of their tasks. They and their representatives shall be subject to the technical supervision of the Information Security Officers the relevant department.

(3) The Information Security Officers the federal administration institutions are responsible for the establishment and maintenance of the Information security process your institution is responsible. They shall draw up an information security policy which shall at least meet the requirements of the Federal Office in accordance with: Section 44(1) requirements. They shall have an impact on the operational implementation of the Information security policy and control the implementation within the institution. The Information security officers advise the management of the establishment of the Federal Administration on all matters relating to information security and inform the management of the federal administration body and the relevant competent authority or authorities. Information Security Officers on a regular basis and on an ad hoc basis, on its activities, on the state of information security within the institution, on resources and staffing and on security incidents. They shall carry out their reporting and advisory tasks independently and without notice.

(4) The Information Security Officers the facilities shall be involved in all activities relating to the information security of the facility. They have a direct right to speak to the respective management of their institution and to the Information Security Officers the relevant department. They may not be dismissed or penalised by their respective institutions for the performance of their tasks.

§ 46

IInformation security officers of the of the departments

(1) The heads of each department and the heads of other supreme federal authorities shall each appoint a Information Security Officers or Information Security Officers the department which, taking into account the needs of IT operations, manages and supervises the Information Security Management within the portfolio or within the supreme federal authority and its area of business, and designate at least one person authorised to represent it. The Information Security Officers the department shall work towards the implementation of information security in its portfolio.

(2) For the performance of their tasks, a targeted capability shall be: the Information Security Officer the portfolio is necessary. The Information Security Officers the department must acquire the expertise necessary for the performance of its tasks.

(3) The Department Information Security Officers coordinate, in each case, the updating of: Information security guidelines for your portfolio. They shall inform the management of their activities and the state of information security within the department, resources and staffing and security incidents. They shall carry out their reporting and advisory tasks independently and without notice.

(4) Justified individual cases may be: or the Information Security Officers the department, in consultation with the relevant IT officer(s) of the department, completely or partially prohibit the use of certain IT products in federal administration facilities within the respective department. The Federal Office shall be informed of any prohibition.

(5) The Information Security Officer of the department, in consultation with the Federal Office, may exempt federal administrative bodies within the department from obligations under this Part, in part or in full, by issuing an exemption decision. The prerequisite for this is that there are objective reasons for issuing an exemption decision and that the exemption does not give rise to any adverse effects on the Federal Government's information security. The Federal Office shall be informed of any exemption decisions issued. The first sentence shall not apply if the relevant body of the federal administration meets the requirements of Section 28(1), first sentence or Section 28 Paragraph 2, first sentence requirements.

(6) The or she: Information Security Officers the department is to be involved in all legislative, regulatory and other important projects within the department in so far as the projects concern information security issues. He or she has a direct right to speak to the respective management of the portfolio. They may not be dismissed or penalised by their respective institutions for the performance of their tasks.

§ 47

Essential digitalisation projects and communication infrastructures of the Federal Government

(1) The planning and implementation of key digitalisation projects and communication infrastructures of the Federal Government are its own Information Security Officers after Section 45 to be appointed.

(2) Digitisation projects or communication infrastructures of the Federal Government are essential, in particular where the federal communication technology is operated across departments or serves cross-ministerial communication or data exchange.

(3) In this rule, the institution appoints the Information Security Officers under the first sentence, which is responsible for the management of the digitisation project or the federal communication infrastructure. In the case of cross-departmental digitisation projects or communication infrastructures, if an order is considered by institutions in different departments involved and other supreme federal authorities and it is not possible to reach agreement within a reasonable period of time on the body by which the order is to be made, the Federal Ministry of the Interior and Community shall decide.

(4) The Information Security Officers in accordance with the first sentence, either the management of the institution or the relevant competent authority or authorities shall: Information Security Officers of the department.

(5) In order to ensure information security in the planning and implementation of major digitisation projects, the responsible body should involve the Federal Office at an early stage and give the Federal Office the opportunity to comment.

§ 48

Office of the Information Security Coordinator

the Federal Government appoints an Information Security Coordinator.

Part 4

Date banks of domain name registration data

§ 49

Obligation to the Maintaining of a database

(1) to contribute to the security, stability and resilience of the Domain Name System, Top Level Domain Name Registries and Domain Name Registration Service Providers shall collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence.

(2) The database shall contain the necessary information to identify and contact the domain name holders and the contact points managing the domain names under the TLD. That information shall cover the following:

1. The domain names;

2. the registration date,

3. The name of the domain holder, his email address and telephone number;

4. The contact e-mail address and telephone number of the contact point that manages the domain names, if different from those of the domain owner.

(3) Top Level Domain Name Registries and Domain Name Registration Service Providers shall have in place policies and procedures, including verification procedures, to ensure that the database contains accurate and complete information. these policies and procedures by [You have*insert: Date, three months after entry into force*] to be made publicly available.

(4) Top Level Domain name Registries and domain name registration service providers shall make the non-personal domain name registration data publicly available without delay after the registration of a domain name.

(5) The Federal Office, compliance with the requirements can be verified.

§ 50

Obligation to the granting of access

(1) Top LevelDomain name Registries and domain name registration service providers shall grant access to domain name registration data without undue delay and in any event within 72 hours of receipt of the request to a legitimate access seeker, upon a reasoned request and to the extent necessary for the performance of their tasks. If the requested information is not available, this shall be notified within 24 hours of receipt of the request for access.

(2) The Top Level Domain Name Registries and Domain Name Registration Service Providers shall have the policies and procedures regarding the disclosure of domain name registration data by [insert: Date, three months after entry into force].

(3) Doha access procedure for inventory data pursuant to Section 22 of the Telecommunications-Digital Services Data Protection Act remains unaffected.

(4) Das Federal Office, compliance with the requirements can be verified.

§ 51

Cooperation obligation

Top Level Domain Name Registries and Domain Name Registration Service Providers shall cooperate to: Section 49 and Section 50 comply with established obligations and in particular to exclude double collection of domain name registration data from the domain holder.

Part 5

Certification, declaration of conformity and marking

§ 52

Crtification

(1) The Federal Office is the national certification body of the Federal Administration for IT Security.

(2) For certain products or services may be requested from the Federal Office for security or personal certification or certification as an IT security service provider. Applications will be processed in the chronological order in which they are received; exceptions may be made if the Federal Office is unable to carry out an examination within a reasonable time because of the number and scope of pending examination procedures and there is a public interest in the grant of a certificate. The applicant must submit to the Federal Office the documents and provide the information the knowledge of which is necessary for the examination and evaluation of the products and performances or the suitability of the person and for the grant of the certificate. A certificate pursuant to sentence 1 may be used for a product, service, person or IT security service provider only if the Federal Office has issued such a certificate and it has not been revoked or otherwise invalidated.

(3) The audit and assessment by the Federal Office in accordance with: Paragraph 7 recognised expert bodies.

(4) The security certificate shall be granted if:

1. Information technology systems, components, products or protection profiles meet the criteria laid down by the Federal Office; and

2. The Federal Ministry of the Interior and Community didn't prohibit the issue of the certificate after paragraph 5.

Before issuing the security certificate, the Federal Office shall submit the file to the Federal Ministry of the Interior and´ for examination in accordance with paragraph 5.

(5) The Federal Ministry of the Interior and Community may prohibit the issue of a certificate in accordance with Paragraph 4 in individual cases, where overriding public interests, in particular security policy interests of the Federal Republic of Germany, preclude the grant.

(6) For the Certification of persons and IT security service providers shall apply mutatis mutandis.

(7) A body as an expert within the meaning of the Paragraph 3 recognised if:

1. The material and human resources and the competence and reliability of the conformity assessment body meet the criteria laid down by the Federal Office, and

2. The Federal Ministry the Interior found that overriding public interests, in particular security policy interests of the Federal Republic of Germany, do not preclude the grant.

The Federal Office ensures, by means of the necessary measures, that the conditions are maintained in accordance with Sentence 1 regularly reviewed.

(8) Certificates issued by other recognised certification bodies in the field of the European Union shall be recognised by the Federal Office, provided that they provide a security equivalent to the Federal Office's security certificates and that equivalence has been established by the Federal Office.

§ 53

Conformity assessment; and Declaration of conformity

(1) For the requirements and guidelines laid down by the Federal Office in a technical guideline, AS Bundesamt may allow a manufacturer or supplier of ICT products, ICT services and ICT processes that do not comply with consumer products in accordance with: Section 55 carry out a self-assessment of its compliance, as well as a person or an IT security service provider. The manufacturer or provider of ICT products, ICT services and ICT processes, the person or the IT security service provider may, subject to the conditions set out in the first sentence, issue a declaration of conformity confirming its compliance with the requirements set out in the Technical Directive. By issuing the declaration of conformity, the manufacturer or provider of the ICT products, ICT services and ICT processes, the individual or the IT security service provider (issuer) shall be responsible for ensuring that the ICT product, ICT service, ICT process, person or IT security service complies with the requirements set out in the Technical Directive. A declaration referred to in the third sentence may only be used for an ICT product, ICT service and ICT process, person or IT security service provider if the manufacturer, provider, person or IT security service provider has issued it and has not been revoked or invalidated in accordance with paragraph 5, point (3).

(2) The technical guidelines referred to in paragraph 1 may, in particular, specify:

1. The content and format of the declaration of conformity;

2. Auxiliaries and procedures to substantiate the information contained in the declaration of conformity;

3. The Conditions for maintaining, maintaining and renewing the declaration of conformity;

4. The use of a label and seal provided by the Federal Office and the conditions for its use;

5. The notification and handling of identified vulnerabilities of the ICT product, ICT service or ICT process or IT security service;

6. Provide information on the Federal Office's website on the declaration of conformity, its issuer and the ICT product, service, process, person or IT security service; or

7. The Limitation of the period of validity of the statement of conformity.

(3) If IRD specifies in paragraph 2 that the information in the declaration of conformity can only be demonstrated by an accredited conformity assessment body, the Federal Office may, upon request, grant a power to conformity assessment bodies intending to operate within the scope of this paragraph if the relevant conditions of the Technical Guidelines are met. Without authorisation from the Federal Office, conformity assessment bodies shall not act within the scope of this paragraph.

(4) The issuer shall keep at the disposal of the Federal Office the declaration of conformity, technical documentation and any other relevant information relating to the conformity of the ICT products, ICT services and ICT processes, person or IT security service with the established criteria for a period specified by the Federal Office in the Technical Guidelines referred to in paragraph 1. A copy of the declaration of conformity shall be submitted to the Federal Office.

(5) The Federal Office may take appropriate measures to ensure that issuers of declarations of conformity comply with the requirements of the scheme and the requirements of this paragraph, and in particular:

1. require declarations of conformity to provide it with all the information necessary for the performance of its tasks;

2. carry out tests in the form of mystery shopping or audits of issuers of declarations of conformity in order to verify their compliance with the requirements and requirements laid down in the Technical Directive in accordance with paragraph 1; and

3. Invalidate declarations of conformity referred to in paragraph 1.

(6) for the measures referred to in paragraph 4, the Federal Office may charge fees if it has acted on the basis of evidence giving rise to reasonable doubts as to compliance with the requirements of the Technical Guideline or this Clause.

§ 54

National cybersecurity certification authority

(1) The Federal Office is the national authority for the Cybersecurity certification in accordance with Article 58(1) of Regulation (EU) 2019/881.

(2) The Federal Office may, upon request, conformity assessment bodies which, within the scope of Regulation (EU) 2019/881 and Section 52 this law confers a power to act as such if the conditions laid down in the relevant European scheme for Cybersecurity certification in accordance with Article 54 of Regulation (EU) 2019/881 or Section 52 this Act has been complied with. Conformity assessment bodies may not operate within the scope of Regulation (EU) 2019/881 without being granted the power to do so by the Federal Office.

(3) Insofar as it is necessary to carry out its tasks under Article 58(7) of Regulation (EU) 2019/881 and Section 52 of this Act, the Federal Office may require conformity assessment bodies to which a power has been granted in accordance with paragraph 2, holders of European cybersecurity certificates and issuers of EU declarations of conformity within the meaning of Article 56(8) of Regulation (EU) 2019/881 to provide the necessary information and other assistance, in particular the production of documents or samples. Section 3 The first and third sentences of paragraph 1 of the Accreditation Body Act paragraph 5.1(i) will apply mutatis mutandis.

(4) The Federal Office may carry out investigations in the form of audits pursuant to Article 58(8), point (b), of Regulation (EU) 2019/881 at conformity assessment bodies that have been granted the power referred to in paragraph 2 of this Article, holders of European cybersecurity certificates and issuers of EU declarations of conformity within the meaning of Article 56(8) of Regulation (EU) 2019/881 in order to verify compliance with the provisions of Title III of Regulation (EU) 2019/881. Section 3 The first to third sentences of paragraph 1 of the Accreditation Body Act paragraph 5.1(i) will apply mutatis mutandis.

(5) The Federal Office shall have the power to enter, inspect and examine documents and templates of conformity assessment bodies to which a power has been granted in accordance with paragraph 2 and of holders of European cybersecurity certificates within the meaning of Article 56(8) of Regulation (EU) 2019/881 during the periods when the spaces are normally available for the relevant business or operational use, to the extent necessary for the performance of their tasks under Article 58(7) of Regulation (EU) 2019/881 and Section 54 of this Act. Section 3 The first to third sentences of paragraph 1 of the Accreditation Body Act paragraph 5.1(i) will apply mutatis mutandis.

(6) The Federal Office may revoke cybersecurity certificates issued by it or cybersecurity certificates issued by a conformity assessment body to which a power has been granted under paragraph 2 in accordance with Article 56(6) of Regulation (EU) 2019/881 or declare EU statements of conformity within the meaning of Regulation (EU) 2019/881 invalid if:

1. of course, those certificates or EU declarations of conformity comply with the requirements set out in Regulation (EU) 2019/881 or a European scheme for the Cybersecurity certification do not comply with Article 54 of Regulation (EU) 2019/881; or

2. the Federal Office is unable to establish compliance pursuant to paragraph 1 because the holder of the European cybersecurity certificate or the issuer of the EU statement of conformity has not complied with its obligations to cooperate pursuant to paragraph 3 or because the latter has obstructed the Federal Office in the exercise of its powers pursuant to paragraph 4 or also, in the case of a holder of a European cybersecurity certificate, pursuant to paragraph 5.

Revoked cybersecurity certificates or invalidated EU statements of conformity referred to in the first sentence shall not be used.

(7) may have powers granted by it in accordance with Paragraph 2 revoked;

1. of course, the conditions of the relevant European scheme for the Cybersecurity certification in accordance with Article 54 of Regulation (EU) 2019/881 or Section 52 this Act is not complied with; or

2. if the Federal Office cannot establish that these conditions have been met because the conformity assessment body is required to cooperate in accordance with its duty of cooperation Paragraph 3 has not complied with it or because the Federal Office, in exercising its powers in accordance with the Paragraphs 4 and 5 with disabilities.

§ 55

Voluntary IT security label

(1) The Federal Office shall introduce a uniform IT security mark to inform consumers about the IT security of products of certain product categories defined by the Federal Office. The IT security mark does not make any statement about the data protection properties of a product.

(2) The IT—Security marks consist of:

1. an assurance from the manufacturer or service provider that the product meets certain IT security requirements for a specified period of time (manufacturer's declaration); and

2. information from the Federal Office about the product's security-relevant IT properties (security information).

(3) The IT-—Security requirements to which the manufacturer's declaration refers are laid down in a standard or standard or from an industry-aligned IT security requirement covering the relevant product category, provided that the Federal Office, in a procedure adopted by means of a statutory ordinance pursuant to: Section 56(2)has determined that the standard or standard or industry-aligned IT security requirement is suitable to reflect sufficient IT security requirements for the product category. There is no entitlement to that determination. If there is no finding pursuant to sentence 1, the IT security requirements are set out in a technical guideline published by the Federal Office which: includes the relevant product category, if the Federal Office has already published such a guideline. Where a product is covered by more than one existing norm, standard, industry-specific IT security requirement or technical guideline identified as appropriate, the requirements shall be governed by the more specific existing norm, standard, industry-specific IT security requirement or technical guideline identified as appropriate.

(4) The IT security mark may only be used for a product if the Federal Office has approved the IT security mark for that product. The Federal Office shall check the approval of the IT security mark for a product at the request of the manufacturer or service provider. The request shall be accompanied by the manufacturer's declaration relating to the product and by all documents supporting the claims made in the manufacturer's declaration. The Federal Office shall confirm receipt of the application and check the plausibility of the manufacturer's declaration on the basis of the attached documents. The plausibility check can also be carried out by a qualified third party commissioned by the Federal Office. The Federal Office may charge an administrative fee for processing the request.

(5) The Federal Office authorise the release of the IT security label for the product in question if:

1. the product is in one of the product categories that the Federal Office has announced in a general decree published in the Federal Gazette;

2. the manufacturer's declaration is plausible and sufficiently supported by the enclosed documents; and

3. any administrative fee charged has been paid.

The approval shall be granted in writing and within a reasonable period of time to be determined in the statutory instrument pursuant to Section 56(2). The exact course of the application procedure and the documents to be enclosed shall be governed by the statutory instrument pursuant to Section 56(2).

(6) Once the Federal Office has granted approval, the label of the IT security mark must be affixed to the respective product or to its outer packaging, insofar as this is possible given the nature of the product. The IT security mark may also be published electronically. If the nature of the product makes it impossible to affix it, the IT security mark must be published electronically. The label of the IT security mark has a reference to an website of the Federal Office where the manufacturer's declaration and security information are available. The exact procedure and the form of the reference shall be laid down in the statutory instrument pursuant to Section 56(2).

(7) At the end of the specified period for which the manufacturer or service provider guarantees compliance with the IT security requirements, or after the manufacturer or service provider has declared the withdrawal to the Federal Office, the release expires. The Federal Office shall include a reference to the expiry of the approval in the safety information.

(8) The Federal Office may check compliance with the requirements for the release of the IT security label for a product. If the verification reveals deviations from the manufacturer's declaration or shortcomings, the Federal Office may take the appropriate measures to protect consumers' trust in the IT security label, in particular:

1. publish the deviations or vulnerabilities in the security information in an appropriate manner; or

2. revoke the approval of the IT security mark.

Paragraph 7, second sentence shall apply accordingly.

(9) Before the Federal Office takes a measure pursuant to Paragraph 8 it shall give the manufacturer or service provider the opportunity to remedy the identified deviations or vulnerabilities within a reasonable period of time, unless serious reasons for the safety of the products require immediate action. This shall not affect the authority of the Federal Office to issue warnings under Section 13.

Part 6

Authorisations on issuing Regulations, restrictions on fundamental rights and reporting obligations of legislative appropriations

§ 56

Authorization to issue executive regulations

(1) The Federal Ministry in agreement with the Federal Ministry of Economic Affairs and Climate Protection, the Interior and Community shall determine, by means of a statutory ordinance which does not require the consent of the Bundesrat, the procedure for issuing security certificates and recognitions in accordance with: Section 52 and its content.

(2) The Federal Ministry of the of the Interior and Community in agreement with the Federal Ministry of Economic Affairs and Climate Protection and the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection, shall determine the details of the design, content and use of the IT security label in accordance with: Section 55in order to ensure a uniform design of the label and a clear recognisability of the labelled information technology products, the details of the procedure for determin-

ing the suitability of industry-aligned IT security policies and the application process for release, including the related deadlines and the documents to be attached, as well as the procedure and design of the reference to safety information.

(3) The Federal Ministry of the Interior and Community shall be determined by regulation which does not require the consent of the Bundesrat, in agreement with the Federal Ministry of Economic Affairs and Climate Action, the Federal Ministry of Finance, the Federal Ministry of Justice, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Defence, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Digital and Transport, the Federal Ministry of Education and Research and the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection, which products, services or processes used by a particularly important body or body Section 30(6) about aCybersecurity certification because they are relevant to the provision of the entity's services and the nature and extent of the entity's risk exposure require the mandatory use of certified products, services or processes in this area.

(4) The Federal Ministry of the Interior and Community shall be determined by regulation which does not require the consent of the Bundesrat, in agreement with the Federal Ministry of Economic Affairs and Climate Action, the Federal Ministry of Finance, the Federal Ministry of Justice, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Defence, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Digital and Transport and the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection, specifying: Section 2, point 24 namedsectors, because of their importance as critical services and their level of supply, which are to be regarded as critical installations within the meaning of this Act. The level of coverage to be considered significant shall be determined on the basis of sector-specific thresholds for each service to be considered critical. Access to files resulting from the creation or modificationNo NG shall be granted to this Regulation.

(5) The Federal Ministry in agreement with the Federal Ministry of Economic Affairs and Climate Action and in consultation with the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Digital and Transport, the Federal Ministry of Defence and the Federal Ministry of the Environment, Nature Conservation, Nuclear Safety and Consumer Protection may determine by means of a statutory ordinance which does not require the consent of the Bundesrat.'when an incident is significant in terms of its technical or organisational causes or its impact on the institution, the State, the economy or the number of people affected by the impact, for the purposes of: Section 2(11)The Federal Ministry may transfer this authorisation to the Federal Office by means of a statutory ordinance. Any implementing acts adopted by the European Commission pursuant to the second subparagraph of Article 23(11) of the NIS 2 Directive that determine the conditions for a significant incident shall take precedence over the statutory ordinance referred to in the first and second sentences in this respect.

(6) The Federal Ministry for the Interior and Community, a statutory ordinance which does not require the consent of the Bundesrat may, in agreement with the Federal Ministry of Health, provide that the Federal Office, in accordance with Section 108 of Book V of the Social Security Code, is to apply to approved hospitals other than that in Section 61(3), fifth sentence namedDate of submission of evidence of compliance with all or all of the Section 61(1) order the above-mentioned obligations.

§ 57

Restriction of basic rights

The confidentiality of telecommunications (Article 10 of the Basic Law) is governed by the Sections 7, 8, 9, 11, 12, 15 and 16 restricted.

§ 58

Federal Office's obligations to provide information

(1) The Federal Office informs the Federal Ministry of the Interior and Community of its activities.

(2) The Notification after Paragraph 1 it also serves to inform the public by the Federal Ministry of the Interior and Community of risks to information technology security, which is carried out at least once a year in a summary report. Section 13 (2) shall apply accordingly.

(3) The Federal Ministry of the Interior and Community Committee of the German Bundestag shall inform the German Bundestag Committee of the application of this Act every calendar year by 30 June of the year following the reporting year. It shall also take into account the further development of the relevant EU law.'

(4) The Federal Office shall submit to the European Union Agency for Cybersecurity, for the first time by 18 January 2025, and every three months thereafter, a summary report containing anonymised and aggregated data on significant incidents, significant cyber threats and near misses which, in accordance with: Section 32 and Section 5(2) reported.

(5) The Federal Office submits for the first time by 17 April 2025 and subsequently every two years

1. The European Commission and the Cooperation Group referred to in Article 14 of the NIS 2 Directive, for each sector and subsector referred to in Annex I or II of the NIS 2 Directive, the number of particularly important entities and entities identified in accordance with: Section 33(1) have been registered; and

2. It provides relevant information on the number of critical installations, the sector and subsector referred to in Annex I or II of the NIS 2 Directive to which they belong, the type of services they provide and the provisions on the basis of which they have been identified.

Part 7

Supervision

§ 59

Independence of the Federal Office

The Federal Office is the competent supervisory authority for compliance with the provisions in Part 3

1. some important and particularly important entities established in the Federal Republic of Germany,

2. operators of critical installations whose critical installations are located on the territory of the Federal Republic of Germany; and

3. Inherited federal administrative bodies.

§ 60

Central competence in the European Union for certain types of institutions

(1) Divergent from Section 59 the Federal Office for DNS Service Providers, Top Level Domain Name Registries, Domain Name Registry Service Providers, Cloud Computing Service Providers, Data Centre Service Providers, Content Delivery Networks, Managed Service Providers, Managed Security Service Providers, as well as providers of online marketplaces, online search engines or social networking platforms only if they have their principal place of business in the European Union in the Federal Republic of Germany. If this is the case, the Federal Office is centrally responsible for the establishment throughout the European Union.

(2) As principal place of business in the European Union, as referred to in paragraph 1, the Member State of the European Union in which the decisions of the body relating to the activities of: Cybersecurity risk management are mainly affected. Where such a Member State cannot be identified or where such decisions are not taken in the European Union, the main establishment shall be the Member State where the cybersecurity measures are implemented. Where such a Member State cannot be identified, the main establishment shall be the Member State where the entity in question has the highest number of employees in the European Union.

(3) If anof the type referred to in paragraph 1 sentence 1 has no establishment in the European Union but offers services within the European Union, it shall be obliged to appoint a representative. The representative must be established in a Member State of the European Union where the entity provides the services. If the representative is established in the Federal Republic of Germany, the Federal Office is responsible for the establishment. If a body of the type of body referred to in the first sentence of paragraph 1 has not appointed a representative within the meaning of this paragraph in the European Union, the Federal Office may declare itself responsible for the body concerned.

(4) The Appointment of a representative by an entity of the Paragraph 1, first sentence this type of entity is without prejudice to any legal action that could be taken against the entity itself.

(5) If the Federal Office has made a request for assistance from another Member State of the European Union to a body responsible for: Paragraph 1, first sentence the Federal Office shall be authorised, within the limits of this request, to take appropriate supervisory and enforcement measures in respect of the entity concerned which provides services in the Federal Republic of Germany or operates an information technology system, component or process. The first sentence shall apply mutatis mutandis to requests for assistance from another Member State of the European Union which is responsible for an entity throughout the European Union if the entity provides services in the Federal Republic of Germany or operates an information technology system, an information technology component or an information technology process.

§ 61

Supervision and enforcement measures for particularly important facilities

(1) The Federal Office may order audits or certifications to be carried out by independent bodies to verify the fulfilment of obligations in relation to individual bodies of particular importance in accordance with: Section 30(1), first sentence, alsoin conjunction with Section 31(1) and (2), first sentence and Section 32 Paragraphs 1 to 3 and Section 38(3) have it carried out.

(2) The Federal Office may, after consulting the institutions and business associations concerned, lay down technical and organisational requirements for the auditing bodies. The determination referred to in the first sentence shall be made by means of a public communication on the website of the Federal Office.

(3) The Federal Office may, at the earliest three years after the entry into force of this Law, provide evidence of compliance with some or all of the requirements laid down in Paragraph 1 order the above-mentioned obligations. In so far as, in accordance with its law, the Federal Office: Paragraph 1 If it has made use of it, it may also require the results of the audits, audits or certifications carried out, including any safety deficiencies identified, and the documentation on which the verification was based. In the case of safety deficiencies, it may require the submission of an appropriate plan of remedial measures in agreement with the competent federal supervisory authority or the other competent supervisory authority. The Federal Office may require the submission of appropriate proof that the deficiencies have been remedied. By way of derogation from the first sentence, the Federal Office may, in accordance with Paragraph 108 of Book V of the Social Security Code, order to produce evidence of the fulfilment of some or all of the obligations referred to in paragraph 1, at the earliest five years after the entry into force of this Law, unless a statutory ordinance pursuant to: Section 56(6) an earlier date is determined.

(4) During the selection, the Federal Office shall take into account the extent of the risk exposure, the size of the facility and the likelihood and severity of possible security incidents and their social and economic impact.

(5) The Federal Office may verify compliance with the requirements of this Act in the case of particularly important institutions. It may use a qualified independent third party to carry out the verification. for the purpose of inspection, important institutions must allow the Federal Office and the persons acting on its behalf to enter the premises during normal operating hours and, on request, provide the relevant records, documents and other documents in an appropriate manner, provide information and provide the necessary assistance. In particular: For the purposes of the verification, the Federal Office shall charge fees and expenses to the relevant particularly important body only if the Federal Office has acted on the basis of evidence which has reasonable doubts as to compliance with the requirements laid down in accordance with: Paragraph 30(1) justified.

(6) The Federal Office may, in consultation with the competent supervisory authority, take necessary measures to prevent or remedy an incident or deficiency with respect to particularly important entities in accordance with: Section 30(1), first sentence and the submission of an appropriate plan of remedial measures and proof of remedial action. Consultation with the competent supervisory authority may be omitted if there is a risk of delay. the Federal Office requires reporting on the measures ordered pursuant to sentence 1 within a reasonable period of time. It may also:

(7) The Federal Office may, in consultation with the competent supervisory authority, issue orders to implement the in Paragraph 1 mentioned obligations. Consultation with the competent supervisory authority may be omitted if there is a risk of delay. order the implementation of specific recommendations formulated in the context of a security audit in individual cases within a reasonable period of time. It can:

(8) The Federal Office may order in respect of particularly important entities:

1. Inform natural or legal persons to whom they provide services or perform activities and who are potentially affected by a significant cyber threat of the nature of the threat and possible mitigation or mitigation measures that those persons may take in response to the threat; and

2. Make publicly available information on breaches of the obligations referred to in paragraph 1 in accordance with requirements laid down by the Federal Office.

(9) Providedrovided that important bodies fail to comply with the Federal Office's orders under this Act, despite setting a deadline, the Federal Office may notify the relevant competent supervisory authority.of particular importance The competent supervisory authority may, where there is a link between enforcement action and order, as a last resort:

1. suspend temporarily, in whole or in part, the authorisation granted to that institution, in accordance with the relevant legislation; and

2. business management is reliable in carrying out the activity they are appointed to carry out (Section 2(13)), temporarily prohibit.

Suspension pursuant to point 1 of the second sentence and the prohibition under point 2 of the second sentence shall be permitted only until the particularly important body complies with the orders of the Federal Office for failure to comply with them.

(10) If the Federal Office implements measures with regard to particularly important institutions, it shall inform the competent federal supervisory authority. The information shall be provided immediately in the case of measures taken in accordance with: Paragraph 6 or 7 in the event of imminent danger and without the agreement of the competent supervisory authority.

(11) If in the course of the supervision of an institution or enforcement of a measure, it finds that a breach of the obligations of this Act gives rise to a manifest personal data breach within the meaning of Article 4(12) of Regulation (EU) 2016/679, which must be notified in accordance with Article 33 of that Regulation, it shall immediately inform the competent supervisory authorities.

(12) Enteties providing services in other Member States of the European Union may also, at the request of the relevant competent supervisory authorities of the Member State, take measures in accordance with: Paragraphs 1 to 11 seizures.

§ 62

Supervision and enforcement measures for important installations

Do facts justify the assumption that an important entity commits to: Section 30(1), first sentence'…' Section 32 Paragraphs 1 to 3 and Section 38(3) not or fails to implement correctly, the Federal Office may verify compliance and take action in accordance with: Section 61 meeting.

§ 63

Vcompulsorily

If the Federal Office imposes periodic penalty payments, by way of derogation from Section 11(3) of the Administrative Enforcement Act up to EUR 100,000.

§ 64

Infringements by Social protection institutions

In the case of infringements against a provision named in Section 65(1) to (4), the second to fourth sentences shall apply. In the case of an offence referred to in sentence 1 above committed by social security institutions sponsored by the Federal Government, the Federal Office shall reach an agreement on the measures to be taken with the supervisory authority responsible for the social security institution. In the event of an offence referred to in sentence 1 by social security institutions sponsored by the federal states, the Federal Office shall inform the competent supervisory authority and propose appropriate measures. The competent supervisory authority shall inform the Federal Office of the initiation and implementation of supervisory measures and shall ensure that they are enforced.'

Part 8

Provisions on fines

§ 65

Provisions on fines

(1) Acts contrary to the lawwho opposes Section 39(1), first sentence in connection with a statutory ordinance pursuant to Section 56(4), first sentence fails to provide proof correctly or completely.

(2) It shall be an administrative offence for any person, who intentionally or negligently acts

1. eintactable position in accordance with

   a) Section 11 paragraph 6, Section 16 Paragraph 1, first sentenceincluding in conjunction with: Section 16(3), Section 17 The first sentence, or Section 39(1), fifth sentence,

   b) Section 14 Paragraph 2, first sentence,

   c) Section 18,Section 40 Paragraph 5, first sentence or to Section 61(3), first sentence or (6), first or third sentence, or paragraph 7, first or third sentence or paragraph 8Yevropes, whether or not combined with: Section 62or

   d) Section 35 Paragraph 1, first sentence or Section 36(2), first sentence

   ,

2. contrary to Section 30(1), first sentence fails to take, fails to take any of the measures referred to therein, or fails to do so correctly, fully or in a timely manner;

3. contrary to Section 30(1), third sentence fails to document compliance, incorrect or complete documentation of compliance;

4. contrary to Section 32(1), first sentence fails to make a notification, fails to do so correctly, fully or in good time;

5. contrary to Section 32(2), second sentence fails to submit a final report, or does not submit it correctly, in full or on time;

6. Contrary to Section 33(1) or (2), first sentence, eachalso in conjunction with a statutory ordinance pursuant to Section 56(4), first sentence‘oropposed to Section 34(1) fails to provide, incorrect, complete or timely information;

7. contrary to Section 33(2), second sentence fails to ensure that it is reachable;

8. contrary to Section 34(2) fails to inform the Federal Office or does not inform the Federal Office correctly, fully or in good time;

9. contrary to contrary to Section 35(2), first sentence, also in conjunction with the second sentence, fails to make a communication, fails to do so correctly, completely or in good time,

10. Contrary to Section 39(1), first sentence in connection with a statutory ordinance pursuant to Section 56(4), first sentence fails to provide proof or fails to provide evidence in good time;

11. contrary to Section 49(3), first sentence does not provide for a requirement or procedure referred to therein;

12. contrary to Section 49(3), second sentence or (4) fails to make available in the prescribed manner or in a timely manner a requirement, process or data referred to therein;

13. contrary to Section 50(1), first sentence does not grant access or does not grant access in a timely manner;

14. contrary to the fourth sentence of Paragraph 52(2), the fourth sentence of Section 53(1), the second sentence of Section 54(6) or the first sentence of Section 55(4), uses a certificate, declaration or sign referred to therein,

15. acts contrary to the second sentence of Section 53(3) or Section 54(2), second sentence, or

16. in contravention of Section 61(5), third sentence does not allow entry into a room referred to therein, does not produce, or does not produce a record, document or document referred to therein, or does not provide information or does not provide information in good faith, incomplete or in good time.

(3) Acts contrary to the lawwho has one in Paragraph 1 commits a designated act negligently.

(4) Acts contrary to the lawwho infringes Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certifica-

tion and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15) by intentionally or negligently

1. fails to make available, correctly, incomplete or not within one month of issue an indication referred to in Article 55(1); or

2. in contravention of Article 56(8), sentence 1, failing to provide information, failing to do so correctly, failing to do so completely or failing to do so immediately after a security breach or irregularity has been identified.

(5) The regulatory offence may be punished,

1. In the cases referred to in paragraph 2(1)(d), (2) to (5) and (9);

   a) particular key institutions according to Section 28(1), first sentence a fine of up to EUR 10 million,

   b) important entities referred to in the Section 28(2), first sentence with a fine of up to EUR 7 million,

2. In the Cases of Paragraph 2, point 1(a) a fine of up to EUR 2 million,

3. In the Cases of Paragraph 1 and point (10) of paragraph 2, with a fine of up to EUR 1 million,

4. In in the cases referred to in paragraph 2(1)(c), (6), (8), (11) to (15) and paragraph 4, with a fine not exceeding five hundred thousand euros, and

5. In the cases referred to in point 1(b) of paragraph 2, points 7 and 16; and Paragraph 3 with a fine of up to hundred thousand euros.

In the cases of Sentence 1, points 2 and 3 the third sentence of Section 30(2) of the Administrative Offences Act shall apply.

(6) In the eventof a particularly important entity for the purposes of the Section 28(1), first sentence with anannual turnover of more than EUR 500 million may, by way of derogation from: Paragraph 5, first sentence, point 1(a) an administrative offence in the cases referred to in paragraph 2(1)(d), (2) to (5) and (9) is punishable by a fine of up to 2 % of the annual turnover.

(7) In the event of a important entity for the purposes of the Section 28(2), first sentence with aannual turnover of more than EUR 500 million may, by way of derogation from: Paragraph 5, point 1(b) an administrative offence in the cases referred to in paragraph 2(1)(d), (2) to (5) and (9) is punishable by a fine of up to 1.4 % of the annual turnover.

(8) An annual turnover for the purposes of the Paragraphs 6 and 7 is the total worldwide turnover of the undertaking to which the particularly important entity or entity belongs during the financial year preceding the infringement.

(9) The administrative authority within the meaning of Section 36(1)(1) of the Administrative Offences Act shall be the Federal Office.

(10) Where the supervisory authorities referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of Regulation (EU) 2016/679, a further fine for an infringement under this Law resulting from the same conduct as the infringement that was subject to the fine referred to in Article 58(2), point (i), of Regulation (EU) 2016/679 shall not be imposed.

Anlage 1

Sectors of particularly important and important entities

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
1	**Energy**		
1.1		Power supply	
1.1.1			Electricity suppliers pursuant to Section 3, point 31c of Energy Industry Act (EnWG)
1.1.2			Electricity distribution grid operators pursuant to Section 3, point 3 of Energy Industry Act (EnWG)
1.1.3			Transmission system operators pursuant to Section 3, point 10 of Energy Industry Act (EnWG)
1.1.4			Generating installations operators pursuant to Section 3, point 18d of Energy Industry Act (EnWG)
1.1.5			Nominated electricity market operators as defined in Article 2, point (8) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
1.1.6			Aggregators pursuant to Section 3, point 1a of Energy Industry Act (EnWG)
1.1.7			Energy storage facilities operators pursuant to Section 3, point 15d of Energy Industry Act (EnWG)
1.1.8			Compensation services providers pursuant to Section 3, point 1b of Energy Industry Act (EnWG)
1.1.9			Operators of a recharging point pursuant to Section 2, point 8 of Charging Station Ordinance (LSV)
1.2		District heating or cooling	
1.2.1			District heating or cooling operators as defined in Section 3, points 19 or 20 of Buildings Energy Act (GEG)
1.3		Fuel and fuel oil supply	
1.3.1			Operators of oil transmission pipelines
1.3.2			Operators of oil production, refining and treatment facilities, storage and transmission
1.3.3			Central stockholding entities as defined in Article 2(f) of Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9)

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
1.4		Gas supply	
1.4.1			Gas distribution system operators pursuant to Section 3, point 8 of Energy Industry Act (EnWG)
1.4.2			Transmission system operators pursuant to Section 3, point 5 of Energy Industry Act (EnWG)
1.4.3			Gas storage system operators pursuant to Section 3, point 6 of Energy Industry Act (EnWG)
1.4.4			LNG system operators pursuant to Section 3, point 9 of Energy Industry Act (EnWG)
1.4.5			Gas suppliers pursuant to Section 3, point 19b of Energy Industry Act (EnWG)
1.4.6			Operators of installations for the extraction of natural gas
1.4.7			Operators of natural gas refining and treatment facilities
1.4.8			Operators of hydrogen production, storage and transmission
2	**Transport and traffic**		
2.1		Air	
2.1.1			Air carriers as defined in Article 3, point (4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72) used for commercial purposes
2.1.2			Airport managing bodies as defined in Article 2, point (2) of Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1), and entities operating ancillary installations contained within airports
2.1.3			Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (OJ L 96, 31.3.2004, p. 1)
2.2		Rail	
2.2.1			Railway infrastructure managers pursuant to

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
			Section 2(6) and (6a) of General Railway Act (AEG), including central entities which schedule train running in advance and handle unexpected events
2.2.2			Railway undertakings pursuant to Section 2(3) of General Railway Act (AEG), including operators of service facilities as defined in Section 2(9) of General Railway Act (AEG)
2.3		Water	
2.3.1			Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6), not including the individual vessels operated by those companies
2.3.2			Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28), including their port facilities as defined in Article 2, point (11) of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
2.3.3			Operator of an installation or system for the safe operation of a waterway as defined in Section 1(6)(1) of the of the Federal Waterways Act (WaStrG)
2.4		Road	
2.4.1			Operators of an installation or traffic control system in road transport, including the entities referred to in Section 1(4), subparagraphs 1, 3 and 4 of the Federal Highways Act (FStrG), such as traffic, operations and tunnel control centres, drainage systems, intelligent traffic systems and specialist centres for information technology and safety in road construction, as well as the telecommunications networks of federal motorways
2.4.2			Operators of Intelligent Transport Systems pursuant to Section 2, point (1) of the Intelligent Transport Systems Act (IVSG).
3	**Finance**		
3.1		Banking	
3.1.1			Credit institutions: Entities whose business is to take deposits or other repayable funds from the public and to grant credits for their own account
3.2		Financial market infrastructures	
3.2.1			Trading venues as defined in Section 2(22) of the Securities Trading Act (WpHG)

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
3.2.2			Central counterparties, which intervene between the counterparties to the contracts traded on one or more markets and thus act as buyers for each seller or as sellers for each buyer
4	**Health**		
4.1.1			Healthcare providers as defined in Directive (EU) 2011/24 of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45)
4.1.2			EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26)
4.1.3			Undertakings carrying out research and development activities of medicinal products pursuant to Section 2 of the Medicinal Products Act (AMG)
4.1.4			Undertakings manufacturing pharmaceutical products according to Section C Division 21 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
4.1.5			Undertakings manufacturing medical devices considered to be critical during a public health emergency ('public health emergency critical devices list') within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1)
5	**Water**		
5.1		Drinking water supply	
5.1.1			Operators of water supply installations as defined in Section 2, point 3 of the Drinking Water Ordinance (TrinkwV), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
5.2		Waste water disposal	
5.2.1			Undertakings collecting, disposing of or treating waste water pursuant to Section 2(1) of the Waste Water Charges Act (AbwAG), excluding undertakings for which the collection and disposal of such waste water is a non-essential part of their general activity.
6	**Digital infrastructure**		
6.1.1			Internet Exchange Point providers

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
6.1.2			DNS service providers, excluding operators of root name servers
6.1.3			Top Level Domain name registries
6.1.4			Cloud computing service providers
6.1.5			Data centre service providers
6.1.6			Content Delivery Networks providers
6.1.7			Trust service providers
6.1.8			Providers of public electronic communications networks
6.1.9			Providers of publicly available telecommunications services
6.1.10			Managed Services Provider
6.1.11			Managed Security Services Provider
7	**Space**		
7.1.1			Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks;

Anlage 2

Sectors of important entities

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
1	**Transport and traffic**		
1.1		Postal and courier services	
1.1.1			Postal service providers pursuant to Section 3, point 15 of the Postal Act (PostG), including providers of courier services
2	**Waste management**		
2.1.1			Undertakings carrying out waste management pursuant to Section 3(14) of the Circular Economy Act (KrWG), excluding undertakings for whom waste management is not their principal economic activity
3	**Manufacture, production and distribution of chemicals**		
3.1.1			Manufacturers and importers as defined in Article 3, points (9) and (11) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1) from chemical substances and mixtures as defined in Article 3, points (1) and (2) of that Regulation, provided that they fall within category 20 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
4	**Production, processing and distribution of food**		
4.1.1			Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1), which are engaged in wholesale distribution and industrial production and processing
5	**Manufacturing**		

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
5.1		Manufacture of medical devices and in vitro diagnostic medical devices	
5.1.1			Undertakings manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1) and undertakings manufacturing in vitro diagnostic medical devices as defined in Article 2, point (2) of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 1) p. 176) with the exception of undertakings manufacturing medical devices classified as critical during a public health emergency pursuant to Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1) (‘Public Health Emergency Critical Devices List’)
5.2		Manufacture of computer, electronic and optical products	
5.2.1			Undertakings carrying out any of the economic activities listed in Section C Division 26 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
5.3		Manufacture of electrical equipment	
5.3.1			Undertakings carrying out any of the economic activities referred to in Section C Division 27 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
5.4		Manufacture of machinery and equipment n.e.c.	
5.4.1			Undertakings carrying out any of the economic activities listed in Section C Division 28 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
5.5		Manufacture of motor vehicles, trailers and semi-trailers	
5.5.1			Undertakings carrying out any of the economic activities listed in Section C Division 29 of the Statistical Classification of

Column A	Column B	Column C	Column D
No	Sector	Industry	Type of entity
			Economic Activities in the European Community (NACE Rev. 2)
5.6		Other transport equipment	
5.6.1			Undertakings carrying out any of the economic activities listed in Section C Division 30 of the Statistical Classification of Economic Activities in the European Community (NACE Rev. 2)
6	**Digital providers**		
6.1.1			Providers of online marketplaces
6.1.2			Providers of online search engines
6.1.3			Providers of social networking services platforms
7	**Research**		
7.1.1			Research organisations

Article 2

Amendment to the Federal Intelligence Service Act

In Section 24(5), sentence 2, of the Federal Intelligence Service Act of 20 December 1990 (Federal Law Gazette (BGBl.) I p. 2954, 2979), as last amended by Article 4 of the Act of 6 May 2024 (Federal Law Gazette (BGBl.) 2024 I) No 149), the words: 'Section 5(7) sentences 2 to 8 of the BSI Act' are replaced by the words 'Section 8 (8), sentences 2 to 8 of the BSI Act'.

Article 3

Amendment to the Security Clearance Check identification Ordinance

In Section 1, point 8 of the Security Clearance Check identification Ordinance of 6 February 2023 (Federal Law Gazette (BGBl.) 2023 I) No (33), the words: 'Section 3(1) sentence 2 subparagraph 1, subparagraph 13 sentence 1 points (b) and (c), subparagraph 15 and subparagraph 18 of the BSI Act' are replaced by the words 'Section 3(1) sentence 2 subparagraph 1, 18 points (b) and (c), 22 and 25 of the BSI Act'.

Article 4

Amendment to the Special Fees Ordinance of the Federal Ministry of the Interior and Community, Building and Community for individually attributable public services within its area of competence

Annex 1, Section 7 of the Special Fees Ordinance of the Federal Ministry of the Interior, Building and Community for individually attributable public services within its area of competence of 2 September 2019 (Federal Law Gazette (BGBl.) I p. 1359), as last amended by: Art. 1 V v. 10.9.2021 I 4229 (Federal Law Gazette (BGBl.) I, p. 4229), is amended as follows:

1. In numbers 1.1.1; 1.1.1.4.1; 1.1.1.4.2; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7, the words 'Section 3(1), sentence 2, subparagraph 5, in conjunction with Section 9(2), sentence 1, and (4) BSIG' are replaced by the words 'Section 3(1), sentence 2, subparagraph 8, in conjunction with Section 52(2), sentence 1, and (4) BSIG'.

2. In subparagraph 1.8, the words: 'Section 3(1), sentence 2, subparagraph 5, in conjunction with Section 9(7) BSIG' are replaced by the words 'Section 3(1), sentence 2, subparagraph 8, in conjunction with Section 52(7) BSIG'.

3. In subparagraph 1.9, the entry: 'Section 3(1), sentence 2, subparagraph 5, in conjunction with Section 9(6) BSIG' are replaced by the entry: 'Section 3(1), sentence 2, subparagraph 8, in conjunction with Section 52(6) BSIG'.

4. In subparagraph 1.10, the entry: ‘Section 3(1), sentence 2, subparagraph 8 BSIG’ are replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 12 BSIG’.

5. In subparagraph 2, the entry: ‘Section 3(1), sentence 2, subparagraph 8 BSIG’ are replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 12 BSIG’.

6. In subparagraph 3, the entry: ‘Section 3(1), sentence 2, subparagraph 9 BSIG’ are replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 13 BSIG’.

7. In subparagraph 4, the words: ‘Section 3(1), sentence 2, subparagraphs 12, 13 and 13a BSIG’ are replaced by the words ‘Section 3(1), sentence 2, subparagraphs 16, 18 and 19 BSIG’.

8. In subparagraph 5, the entry: ‘Section 3(1), sentence 2, subparagraph 14 BSIG’ are replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 20 BSIG’.

9. In subparagraph 6, the words: ‘Section 3(1), sentence 2, subparagraph 14a, in conjunction with Section 9c(5) BSIG’ are replaced by the words ‘Section 3(1), sentence 2, subparagraph 21, in conjunction with Section 55(5) BSIG’.

10. In subparagraph 7, the words: ‘Section 3(1), sentence 2, subparagraph 17, in conjunction with Section 8a(2) BSIG’ are replaced by the words ‘Section 3(1), sentence 2, subparagraph 24, in conjunction with Section 39 BSIG’.

11. In subparagraph 8, the entry: ‘Section 3(1), sentence 2, subparagraph 17, in conjunction with Section 8a(3), sentence 4 BSIG’ is replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 24 BSIG in conjunction with Section 39(1)’.

12. In subparagraph 9, the words: ‘Section 3(1), sentence 2, subparagraph 18, in conjunction with Section 5b BSIG’ are replaced by the words ‘Section 3(1), sentence 2, subparagraph 25, in conjunction with Section 11 BSIG’.

13. In subparagraph 10, the entry: ‘Section 3(1), sentence 2, subparagraph 19 BSIG’ are replaced by the entry: ‘Section 3(1), sentence 2, subparagraph 26 BSIG’.

Article 5

Amendment to the Telecommunications Digital Services Data Protection Act

In Section 19 of the Telecommunications Digital Services Data Protection Act of 23 June 2021 (Federal Law Gazette (BGBl.) I, p. 1982; 2022 I p. 1045), as last amended by Article 8 of the Act of 6 May 2024 (Federal Law Gazette (BGBl.) 2024 I) No 149)the entry: ‘Section 7d, sentence 1, of the BSI Act’ is replaced by the entry ‘Section 17, sentence 1, of the BSI Act’.

Article 6

Amendment to the Gender Equality Officer Election Ordinance

In Section 19(9) of the Gender Equality Officer Election Ordinance of 17 December 2015 (Federal Law Gazette (BGBl.) I, p. 2274), as amended by Article 3 of the Act of 7

August 2021, the entry: ‘Section 9 of the BSI Act’ is replaced by ‘Section 52 of the BSI Act’.

Article 7

Amendment to the Second Act on Increasing the Security of Information Technology Systems

Article 6(1) of the Second Act on Increasing the Security of Information Technology Systems of 18 May 2021 (Federal Law Gazette (BGBl.) I, p. 1122, 4304) is amended as follows:

1. The number designation ‘1.’ is deleted and the word ‘and’ following the entry: ‘(Article 1)’ is replaced by a full-stop ‘.’.

2. Subparagraph 2 is repealed.

Article 8

Amendment to the BSI Certification and Recognition Ordinance

The BSI Certification and Recognition Ordinance of 17 December 2014 (Federal Law Gazette (BGBl.) I p. 2231), as last amended by Article 74 of the Regulation of 19 June 2020 (Federal Law Gazette (BGBl.) I p. 1328) is amended as follows:

1. The introductory formula is worded as follows:

   ‘By virtue of Section 56(1) of the BSI Act, as amended and promulgated on [*insert: date and reference of this Act*), the Federal Ministry of the Interior and Community, after consultation with the business associations concerned and in agreement with the Federal Ministry of Economic Affairs and Climate Protection, hereby decrees:’.

2. In Section 1, the entry: ‘Section 9 of the BSI Act’ is replaced by ‘Section 52 of the BSI Act’.

3. In Section 12(1), the entry: ‘Section 9(4) of the BSI Act’ is replaced by the entry: ‘Section 52(4) of the BSI Act’.

4. In Section 15(1) and Section 18(1), the entry ‘Section 9(5) of the BSI Act’ is replaced by the entry: ‘Section 52(6) of the BSI Act’ and the entry ‘Section 9(4)(2) of the BSI Act’ is replaced by the entry: ‘Section 52(4)(2) of the BSI Act’.

5. Section 21 is amended as follows:

   a) In paragraph 1, the entry: ‘Section 9(6) of the BSI Act’ is replaced by the entry: ‘Section 52(7) of the BSI Act’.

   b) In paragraph 1, subparagraph 2, the entry: ‘Section 9(6)(2) of the BSI Act’ is replaced by the entry: ‘Section 52(7), sentence 1, subparagraph 2 of the BSI Act’.

   c) In paragraph 4, sentence 1, the entry: ‘Section 9(6), sentence 2 of the BSI Act’ is replaced by the entry: ‘Section 52(7), sentence 2, of the BSI Act’.

Article 9

Amendement to the BSI IT Security Label Ordinance

The BSI IT Security Label Ordinance of 24 November 2021 (Federal Law Gazette (BGBl.) I, p. 4978) is amended as follows:

1. The introductory formula is worded as follows:

   'By virtue of Section 56(2) of the BSI Act, as amended and promulgated on … [insert: date and reference of this Act], the Federal Ministry of the Interior and Community, in agreement with the Federal Ministry of Economic Affairs and Climate Protection and the Federal Ministry of Justice and the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection, hereby decrees:'.

2. In Section 2, subparagraph 4, the entry: 'Section 9c(3), sentence 1, of the BSI Act' is replaced by 'Section 55(3), sentence 1, of the BSI Act'.

3. In Section 3(1), sentence 1, the entry 'Section 9c(2) of the BSI Act' is replaced by 'Section 55(2) of the BSI Act'.

4. Section 5 is amended as follows:

   a) In paragraph 4, the entry: 'Section 9c(5) BSIG' is replaced by 'Section 55(5) of the BSI Act'.

   b) In paragraph 5, sentence 1, the entry: 'Sections 7 or 7a of the BSI Act' is replaced by 'Section 13 or 14 of the BSI Act' and the entry: 'Section 9c(8) of the BSI Act' is replaced by the entry 'Section 55(8) of the BSI Act'.

5. In Section 6(1), the entry: 'Section 9 of the BSI Act' is replaced by the entry 'Section 52 of the BSI Act'.

6. In Section 7(3) and Section 9(1), sentence 1, the entry 'Section 9c of the BSI Act' is replaced by the entry 'Section 55 of the BSI Act'.

7. Section 13 is amended as follows:

   a) In sentence 1, the entry 'Section 9c(2) of the BSI Act' is replaced by the entry 'Section 55(2) of the BSI Act'.

   b) In sentence 2, the entry: 'Sections 7 or 7a of the BSI Act' is replaced by 'Section 13 or 14 of the BSI Act'.

8. In Section 14, the entry: 'Section 10(3), sentence 1, of the BSI Act' is replaced bythe entry 'Section 56(2) of the BSI Act'.

Article 10

Amendment to the De-Mail Act

In Section 18(3)(3) of the De-Mail Act of 28 April 2011 (BGBl. I p. 666), as last amended by Article 10 of the Act of 6 May 2024 (Federal Law Gazette (BGBl.) 2024 I) No 149), the words: 'Section 9(2), sentence 1, of the Act on the Federal Office for Information Security' is replaced by the words 'Section 52(2), sentence 1, of the BSI Act'.

Article 11

Amendment to the e-Government Act

In Section 10 of the e-Government Act of 25 July 2013 (Federal Law Gazette (BGBl.) I p. 2749), as last amended by Article 1 of the Act of 16 July 2021 (Federal Law Gazette (BGBl.) I p. 2941), the sentence 2 is repealed.

Article 12

Amendment to the Passport Data Acquisition and Transmission Ordinance

In Section 4(2) of the Passport Data Acquisition and Transmission Ordinance of 9 October 2007 (Federal Law Gazette (BGBl.) I, p. 2312), as last amended by Article 4 of the Regulation of 30 October 2023 (Federal Law Gazette (BGBl.) 2023 I No 290), the words: 'Section 9 of the BSI Act of 14 August 2009 (Federal Law Gazette (BGBl.) I, p. 2821)' are replaced by the words: 'Section 52 of the BSI Act of … [insert: date and reference of this Act]'.

Article 13

Amendment of the ID Card Ordinance

In Section 3(2) of the ID Card Ordinance of 1 November 2010 (BGBl. I, p. 1460), as last amended by Article 2 of the Regulation of 12 April 2024 (Federal Law Gazette (BGBl.) 2024 I) No 125), the words: 'Section 9 of the BSI Act of 14 August 2009 (Federal Law Gazette (BGBl.) I, p. 2821), as last amended by Article 1 of the Act of 23 June 2017 (Federal Law Gazette (BGBl.) I p. 1885), ARE replaced by the entry 'Section 52 of the BSI Law of … [insert: date and reference of this Act]'.

Article 14

Amendment to the Whistleblower Protection Act

In Section 2(1)(3)(q) of the Whistleblower Protection Act of 31 May 2023 (Federal Law Gazette (BGBl.) 2023 I) No 140), the entry: 'Section 2(2) of the BSI Act' is replaced by the entry: 'Section 2(39) of the BSI Act' and thewords 'of the digital providers as defined in Section 2(12) of the BSI Act' are replaced by the words: 'particularly important entities pursuant to Section 28(1) of the BSI Act and important entities pursuant to Section 28(2) of the BSI Act, in so far as they fall within the types of entities pursuant to Annex 1 subparagraph 6.1.4. or Annex 2 subparagraph 6.1.1. or 6.1.2 of the BSI Act'.

Article 15

Amendment to the Cash Register Anti-Tampering Ordinance

In Section 11(1) of the Cash Register Anti-Tampering Ordinance of 26 September 2017 (Federal Law Gazette (BGBl.) I p. 3515), as amended by Article 2 of the Regulation of 30 July 2021 (Federal Law Gazette (BGBl.) I p. 3295)the entry 'Section 9 of the BSI Act' is replaced by the entry 'Section 52 of the BSI Act'.

Article 16

Amendement to the Atomic Energy Act

In Section 44b of the Atomic Energy Act, as amended and promulgated on 15 July 1985 (Federal Law Gazette (BGBl.) I p. 1565), as last amended by Article 1 of the Act of 4 December 2022 (Federal Law Gazette (BGBl.) I p. 2153), the entry: 'Section 8b paragraphs (1), (2) subparagraphs (1) to (3), (4) points (a) to (c) and paragraph (7) of the BSI Act' is replaced by 'Section 40 paragraphs (1), (3) subparagraphs (1), (2), (3), (4) points (a), (d) and paragraph (6) of the BSI Act'.

Article 17

Amendment to the Energy Industry Act

The Energy Industry Act of 7 July 2005 (Federal Law Gazette (BGBl.) I p. 1970, 3621), as last amended by Article 1 of the Act of 14 May 2024 (Federal Law Gazette (BGBl.) 2024 I) No 161), is amended as follows:

1. In the table of contents, the following reference to Section 5c is inserted after the reference to Section 5b:

   'Section 5c IT security in plant and network operations, defining competence'.

1. After Section 5b, the following Section 5c is inserted:

‘Section 5c

IT security in plant and network operations, defining competence

(1) The operator of an energy supply network must ensure adequate protection against threats to telecommunication systems and electronic data processing systems that are necessary for secure network operation. The appropriate protection under the sentence 1 shall also be ensured by taking into account the necessary requirements in the procurement of fixed assets and services. The Federal Network Agency, in consultation with the Federal Office for Information Security, shall determine the requirements for appropriate protection in a catalogue of security requirements (IT security catalogue) in accordance with Section 29(1). In doing so, the Federal Network Agency shall involve the operators of energy supply networks and their industry associations. The Federal Network Agency reviews the IT security catalogue every two years and updates it as necessary. Adequate protection under sentence 1 exists: if the IT Security Catalogue requirement is complied with. Compliance with the requirements of the IT sSecurity Catalogue must be documented by the operator.

(2) The operator of an energy installation which is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act of… [insert: date and reference to in Article 1], as amended, or an important entity referred to in Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network must ensure adequate protection against threats to telecommunications systems and electronic data processing systems necessary for secure system operation. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected. The appropriate protection under the sentence 1 shall also be ensured by taking into account the necessary requirements in the procurement of fixed assets and services. The Federal Network Agency, in consultation with the Federal Office for Information Security, shall determine the requirements for appropriate protection in a IT security catalogue in accordance with Section 29(1). In doing so, the Federal Network Agency shall involve the operators referred to in sentence 1 and their industry associations. The Federal Network Agency reviews the IT security catalogue every two years and updates it as necessary. For telecommunications systems and electronic data processing systems of installations pursuant to Section 7(1) of the Atomic Energy Act, as amended and promulgated on 15 July 1985 (Federal Law Gazette (BGBl.) I p. 1565), as last amended by Article 16 of the Act of … [insert: date and reference to in Article 33(1),sentence 1], requirements under the Atomic Energy Act take precedence over the requirements of the IT Security Catalogue pursuant to sentence 4. The licensing and supervisory authorities of the Federal Government and the Länder responsible for nuclear safety shall be involved in the development of the IT security catalogue pursuant to sentence 4. Appropriate protection under sentence 1 shall be deemed to exist if the requirements of the IT security catalogue are complied with. Compliance with the requirements of the IT security catalogue must be documented by the operator.

(3) IT-security catalogue referred to in paragraph 1, sentence 3 and the IT security catalogue referred to in paragraph 2, sentence 4 shall each respect the state of the art and ensure a level of security of the information technology systems, components and processes appropriate to the risk, taking into account the relevant European standards or international standards and the compliance costs. When assessing whether measures are proportionate to the risk involved, account shall be taken of the extent of the risk exposure and the size of the operator, as well as the likelihood and severity of security incidents, as well as their societal and economic impact. The IT security catalogue referred to in paragraph 1, sentence 3 and the IT security catalogue referred to in paragraph 2, sentence 4 shall in each case include at least the following:

1. concepts on risk evaluation and information technology security;

2. the management of security incidents;

3. maintaining operations, such as backup management and post-emergency recovery, and crisis management;

4. the security of the supply chain, including security-related aspects of the relationship between each entity and its immediate suppliers or service providers;

5. security measures in the acquisition, development and maintenance of network and information systems, including vulnerability management and disclosure;

6. cincepts and procedures for assessing the effectiveness of information technology security risk management measures;

7. basic procedures in the field of cyber hygiene and training in the area of information technology security;

8. concepts and procedures for the use of cryptography and encryption;

9. sstaff security, access control and facility management concepts;

10. the use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communication and, where appropriate, secured emergency communication systems within the entity;

11. the use of attack detection systems according to Section 2(41) of the BSI Act,

12. the use of an element or group of elements of a network or information system (ICT product), of a service consisting wholly or mainly of the transmission, storage, retrieval or processing of information by means of network and information systems (ICT service) and any activity aimed at designing, developing, providing or maintaining an ICT product or service (ICT process) with cybersecurity certification under European schemes pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (OJ 151, 7.6.2019, p. 15).

The Federal Network Agency may make more detailed provisions in the IT security catalogues on the format, content and design of the documentation required under paragraph 1, sentence 7 or paragraph 2, sentence 10 on compliance with the requirements of the relevant IT security catalogue and on the resolution of security deficiencies. The Federal Network Agency may also include rules in the IT security catalogues for the regular verification of compliance with the security requirements.

(4) The operator of an energy supply network or the operator of an energy installation which is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network shall submit to the Federal Network Agency the documentation on compliance with the requirements of the relevant IT security catalogue pursuant to paragraph 1, sentence 7 or paragraph 2, sentence 10. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected. If necessary, the Federal Network Agency may request the submission of the plan of remedial measures from the operator in accordance with sentence 1. In the event of safety deficiencies arising from the plan of remedial measures, the Federal Network Agency may require the operator pursuant

to sentence 1 to remedy those deficiencies within a time limit set by the Federal Network Agency. For the purpose of verifying compliance with the safety requirements under paragraph 1 or paragraph 2, the operator referred to in sentence 1 shall allow the Federal Network Agency and the persons acting on its behalf to enter the business and operational premises during normal operating hours and, on request, submit the relevant records, documents and other documents in an appropriate manner, provide information and grant the necessary assistance. For the purposes of the review, the Federal Network Agency shall levy fees and expenses only if the Federal Network Agency has acted on the basis of indications that give rise to reasonable doubts as to compliance with the requirements set out in paragraphs 1 and 2.

(5) If the Federal Network Agency is aware of any information or information indicating that an operator of an energy installation who is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network which fails to implement or does not correctly implement the security requirements referred to in paragraph 2, it may request information from that operator in order to verify compliance with the security requirements referred to in paragraph 2. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected. Paragraph 4, sentences 3 to 6, applies accordingly.

(6) The operator of an energy supply network or the operator of an energy installation which is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network is obliged to report the following information to a joint reporting unit set up by the Federal Office for Information Security and the Federal Office for Civil Protection and Disaster Assistance:

1. without delay and at the latest within 24 hours of becoming aware of a significant incident in accordance with Section 2(11) of the BSI Act, an early initial notification indicating whether there is a suspicion that the significant incident is due to an illegal or malicious act or may have a cross-border impact;

2. without delay and at the latest within 72 hours of becoming aware of a significant incident in accordance with Section 2(11) of the BSI Act, a significant incident notification confirming or updating the information referred to in suparagraph 1 and indicating an initial assessment of the significant incident, including its severity and impact, and, where applicable, the compromise indicators;

3. at the request of the Federal Office for Information Security an interim report of relevant status updates;

4. no later than one month after the notification of the significant incident has been submitted in accordance with Section 2(11) of the BSI Act, a final report containing:

a) a detailed description of the significant incident in accordance with Section 2(11) of the BSI Act, including its severity and impact;

b) information on the nature of the threat or underlying cause that is likely to have triggered the significant incident in accordance with Section 2(11) of the BSI Act;

c) information on the corrective measures taken and on-going;

d) if necessary, the cross-border impact of the significant security incident pursuant to Section 2(11) of the BSI Act.

Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected. Section 32 (2) to (5) and Section 36 of the BSI Act shall apply accordingly. In the case of reports under this paragraph, the Federal Office for Information Security shall take measures pursuant to Section 36 of the BSI Act in consultation with the Federal Network Agency.

(7) The Federal Office for Information Security shall submit the reports referred to in paragraph 6 and such reports of security incidents in accordance with Section 32 forward the BSI Act to the Federal Network Agency without delay, in which the Federal Office for Information Security becomes aware of the relevance for the security of energy supply and fulfilment of the purposes and objectives referred to in Section 1. The Federal Network Agency shall without delay carry out an assessment of the impact of the security of energy supply submitted pursuant to sentence 1 and transmit its results to the Federal Office for Information Security. The Federal Network Agency may require the undertaking concerned to provide the information necessary to assess the impact of the incident on energy security, including personal data, and has the power to collect, store and use personal data necessary to assess the impact of the incident on energy security. The undertaking concerned must provide the Federal Network Agency with the information necessary to assess the impact of the incident on energy security, including personal data. In carrying out the assessment referred to in sentence 2, the Federal Network Agency may involve transmission, long-distance transmission and distribution networks operators and shall have the power to provide them with the personal data necessary for that purpose. Transmission, long-distance transmission and distribution networks operators shall have the right to collect, store and use the personal data transmitted to them pursuant to sentence 5 for the purposes specified therein. Once the assessment has been drawn up, the personal data used for this purpose must be deleted by the Federal Network Agency and the operators of transmission, long-distance transmission and distribution networks without delay. The Federal Office for Information Security shall take into account the assessment of the Federal Network Agency when carrying out its tasks under Section 40(3)(2) of the BSI Act. The Federal Office for Information Security and the Federal Network Agency shall ensure that unauthorised disclosure of the information of which they have become aware pursuant to sentence 1 is excluded. Access to the files of the Federal Office for Information Security and to the files of the Federal Network Agency in matters pursuant to paragraphs 1 to 6 and this paragraph shall not be granted. Section 29 of the Administrative Procedure Act shall remain unaffected.

(8) The operator of an energy supply network or an energy installation which is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network is obliged to submit the information referred to in Section 33(1)(1) to (4) of the BSI Act to the Federal Office for Information Security by means of a registration facility jointly established by the Federal Office for Information Security and the Federal Office for Civil Protection and Disaster Assistance, no later than three months no later than three months after it is deemed to be one of the aforementioned entities for the first time or again. The operator of an energy supply network which is not a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or not an important entity under Section 28(2), sentence 1 of the BSI Act is obliged to provide, by the end of … [insert: the date of the day of the third calendar month following the month of entry into force pursuant to Article 33(1), sentence 1, whose number is the same as that of the day of entry into force pursuant to Article 33(1), sentence 1, or, if there is no such calendar day, the date of the first day of the following calendar month] the Federal Office for Information Security through a registration facility jointly established by the Federal Office for Information Security and the Federal Office for Civil Protection and Disaster Assistance, the information in accordance with Section 33(1)(1) to (4) of the BSI Act. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains un-

affected. Section 33 (2), (4) and (5) the BSI Act shall apply accordingly. The Federal Office for Information Security shall transmit the registrations referred to in sentences 1 and 2, including the associated contact details and any changes to the registrations, to the Federal Network Agency without delay. The Federal Office for Information Security may also carry out the registrations referred to in sentences 1 and 2 itself and designate a contact point if the operator fails to fulfil its obligation to register. If the Federal Office for Information Security itself makes such a registration, it shall inform both the operator concerned and the Federal Network Agency thereof and provide the associated contact details. Each operator must ensure that it can be contacted at all times via the contact point designated or specified by the Federal Office for Information Security. The transmission of information by the Federal Office for Information Security in accordance with Section 40(3)(4)(a) of the BSI Act shall be made to this contact point.

(9) Business managers of an operator of an energy supply network or of an energy installation operator carrying out a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network shall be obliged to implement the security requirements referred to in paragraphs 1 or 2 and to monitor their implementation. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected.

(10) Business managers who fail to comply with their obligations under paragraph 9 shall be liable for any damage caused to their entity in accordance with the company law rules applicable to the legal form of the entity. Under that Act, they are liable only if the company law provisions governing the entity do not contain any liability regime under sentence 1.

(11) Business managers of an operator of an energy supply network or an operator of an energy installation which is a particularly important entity in accordance with Section 28(1), sentence 1 of the BSI Act or an important entity under Section 28(2), sentence 1 of the BSI Act and whose energy installation is connected to an energy supply network must undergo regular training in order to acquire sufficient knowledge and skills to identify and assess risks and risk management practices in the field of information technology security and to assess the impact of risks and risk management practices on the services provided by the entity. Section 28 (1), sentence 2 and Section 28(2), sentence 2 of the BSI Act remains unaffected.

(12) By the end of… [insert: the date of the day of the third calendar month following the month of entry into force pursuant to Article 33(1), sentence 1, whose number is the same as that of the day of entry into force pursuant to Article 33(1), sentence 1, or, if there is no such calendar day, the date of the first day of the following calendar month], the Federal Network Agency shall specify, in agreement with the Federal Office for Information Security, by means of a general order, in accordance with Section 29(1), in a catalogue of safety requirements for the operation of energy supply networks and energy installations,

1. which components are critical components according to Section 2(23)(c)(aa) of the BSI Act, or

2. which functions are critically defined functions according to Section 2(23)(c)(bb) of the BSI Act.

The operator of an energy supply network which is a critical facility within the meaning of Section 2(22) of the BSI Act or the operator of an energy installation which is a critical facility within the meaning of Section 2(22) of the BSI Act shall comply with the requirements of the Catalogue no later than six months after its entry into force as spec-

ified in the General Order, unless a different transposition period has been laid down in the catalogue. The catalogue shall be connected to the IT security catalogues referred to in paragraphs 1 and 2.'

1. Section 11 Paragraphs 1a to 1g are repealed.

2. Section 59 (1), point 1a is replaced by the following:

'1a. the provisions pursuant to Section 5c(1), (2) and (12),'.

3. Ipoint 4 of the first sentence of Section 91(1) shall be inserted after the words: 'Official acts on the basis of Paragraphs' the indication: '5c(4),'; shall be added.

4. Section 95 is amended as follows:

a) Paragraph 1 shall be amended as follows:

a%6) Dpoints 2a and 2b of IE are deleted.

b%6) Nin point 3a, the following points 3b, 3c and 3d are inserted:

'3b. fails to ensure the protection referred to therein, contrary to the first sentence of Paragraph 5c(1) or the first sentence of paragraph 2,

3c. fails to document compliance with the requirements of the IT Security Catalogue or does not correctly or fully document compliance with the requirements of the IT Security Catalogue, contrary to Section 5c(1), seventh sentence or (2), sentence 10;

3d. fails to make a notification, incorrect, incomplete or timely, contrary to the first sentence of Section 5c(6),';

c%6) Dpoints 3b to 3d are renumbered 3e to 3g.

d%6) Dpoints 3f to 3i are renumbered as points 3h to 3k.

b) Nin paragraph 2, the following paragraphs 2a to 2d are inserted:

'(2a) The administrative offence may be punished in the cases referred to in points 3b to 3d of paragraph 1:

1. in the case of particularly important facilities: Section 28(1) First sentence of the BSI Act, with a fine of up to EUR 10 million,

2. in the case of important facilities, see: Section 28(2) The first sentence of the BSI Act, with a fine of up to EUR 7 million, and

3. in other cases, a fine of up to EUR 1 million.

(2b) In the case of a particularly important entity within the meaning of the Section 28(1) The first sentence of the BSI Act with an annual turnover of more than EUR 500 million may, by way of derogation from paragraph 2a(1), be punishable by an administrative offence under subparagraph 1(3b), (3c) and (3d) by a fine of up to 2 % of the annual turnover.

(2c) In the case of an important entity within the meaning of the Section 28(2) The first sentence of the BSI Act with an annual turnover of more than EUR 500 million may, by way of derogation from paragraph 2a(2), be punishable

by an administrative offence under subparagraph 1(3b), (3c) and (3d) by a fine of up to 1.4 % of the annual turnover.

2d Section 65 Paragraph 8 the BSI Act shall apply mutatis mutandis.'

c) IN paragraph 5 is renumbered as: shall be replaced by 'Point 2b''Point 3d'.

Article 18

Amendment to the Measuring Point Operation Act

In Section 24(2) of the Measuring Station Operation Act of 29 August 2016 (BGBl. I, p. 2034), as last amended by Article 7 of the Act of 8 May 2024 (BGBl. 2024 I) No. 151) has been amended;'if the words: 'Section 9 of the BSI Act of 14 August 2009 (BGBl. I, p. 2821)' there shall be substituted: 'Paragraph 52 of the BSI Law of… [insert: Date and reference of Article 1] in its up-to-date version'.

Article 19

SIMILARNon-compliance with Energy Security Act

The Energy Security Act of 20 December 1974 (BGBl. I, p. 3681), as last amended by Article 1 of the Act of 23 June 2023 (BGBl. 2023 I) No. 167) has been amended, is amended as follows:

1. The following sentence is added to § 10(1):

   'In so far as data within the meaning of the third sentence for measures pursuant to Section 1 of the Gas Security Regulation of 26 April 1982 (BGBl. I p. 517), as last amended by Article 1 of the Ordinance of 31 March 2023 (BGBl. 2023) No. (94) and, for solidarity measures pursuant to Section 2a, the Federal Network Agency shall transmit the data to the Federal Financial Supervisory Authority at its request and to the extent necessary for the performance of its tasks.'

2. IN Section 17(1), Section 18(2), first sentence, point 1, and Section 29(1), first sentence, shall be replaced by the words 'Critical Infrastructure' means there shall be substituted: 'critical installations' means: and the words 'Section 2(10) of the BSI Act' through the words 'Section 2(22) of the BSI Act'.

Article 20

Amendment to the Heat Planning Act

In the first sentence of Section 11(4) of the Heat Planning Act of 20 December 2023 (BGBl. 2023 I) No. 394)'if the words: 'Critical infrastructure' means: there shall be substituted: 'critical installations' and the words 'Section 2(10) of the BSI Act of 14 August 2009 (BGBl. I, p. 2821), as last amended by Article 12 of the Act of 23 June 2021 (BGBl. I, p. 1982)' there shall be substituted: 'Paragraph 2(22) of the BSI Law of… [insert: Date and reference of Article 1] in its up-to-date version'.

Article 21

Amendments to Volume V of the German Social Code

Book Fifth of the Social Security Code – Statutory Health Insurance (Article 1 of the Law of 20) December 1988, BGBl. I pp. 2477, 2482), as last amended by Article 3 of the Act of 30 May 2024 (BGBl. 2024 I) No. 173) has been amended;‘is amended as follows:

1. Section 391 is amended as follows:

   a) IN paragraph 4 the words: there shall be substituted: ‘Section 8a(2) of the BSI Act’ ‘Section 30(8) of the BSI Act’.

   b) IN paragraph 5 shall read the words: ‘Critical infrastructure’ means: there shall be substituted: ‘critical installations’ means: and the words ‘Section 8a of the BSI Act’ there shall be substituted: ‘Section 30, 31 and 39 of the BSI Act’.

2. Section 392 is amended as follows:

   a) IN paragraph 3 shall read the words: ‘Section 8a(2) of the BSI Act’ there shall be substituted: ‘Section 30(8) of the BSI Act’.

   b) IN paragraph 5 shall read the words: ‘Critical infrastructure’ means: there shall be substituted: ‘critical installations’ means: and the words ‘Section 8a of the BSI Act’ there shall be substituted: ‘Section 30, 31 and 39 of the BSI Act’.

Article 22

Amendment to the Digital Health Applications Regulation

In Appendix 1 to the Digital Health Applications Ordinance of 8 April 2020 (BGBl. I p. 768), as last amended by Article 4 of the Act of 22 March 2024 (BGBl. 2024 I) No. (101)‘are included in the section: ‘Data security’ means:Sub-section ‘Basi requirements applicable to all digital health applications’ in point 5 in the column: ‘Requirement’ the words ‘The first sentence of Paragraph 8(1) of the BSI Act’ through the words ‘Section 44 Paragraph 1, first sentence the BSI Act’.

Article 23

SIMILARnon-compliance with Book 6th Social Code

Book 6 of the Social Security Code – Statutory Pension Insurance – in the version published on 19 February 2002 (BGBl. I, pp. 754, 1404, 3384), as last amended by Article 1 of the Act of 30 May 2024 (BGBl. 2024 I) No. 173) has been amended;‘is amended as follows:

1. The table of contents is amended as follows:

   a) After the entry for § 145, the following entry is inserted:

‘Subsection 8

Security in information technology’.

b) The entry for § 146 is worded as follows:

Section 146: Binding decisions on the security of information technology’.

2. Section 138 Sentence 2 of Paragraph 1 is amended as follows:

a) IN point 15 is renumbered after the word: ‘Rehabilitation’ there shall be deleted: ‘and’ replaced by a comma.

b) In point 16, the full stop at the end is replaced by the word ‘and’.

c) The following subparagraph 17 is added:

1. ‘ Coordination of information technology in the field of pension insurance in line with the objectives of efficiency and security.’

3. N(Ach Section 145) the following heading is inserted:

‘Subsection 8

Information technology security’.

4. § 146 is worded as follows:

§ 1‘

Vbinding decisions on the security of information technology

The Deutsche Rentenversicherung Bund shall, in the performance of the tasks assigned to it under Section 138(1), second sentence, point 17, take the following binding decisions by 30 June 2025:

1. Zestablishing uniform principles for information technology and information security for pension insurance;

2. Zthe operation of the information technology infrastructure and the network of pension insurance;

3. Zdevelopment of pension-related applications; and

4. Zdefinition of a procurement concept.

The first sentence shall apply in relation to the Deutsche Rentenversicherung Knappschaft-Bahn-See, with the proviso that necessary derogations may be made because of the further statutory tasks entrusted to it and their specific benefits.’

Article 24

Amendment to the Ordinance on the Accessibility Enhancement Act

In Section 2(3) of the Regulation on Accessibility Enhancement Act of 15 June 2022 (BGBl. I p. 928) the words: ‘Section 2(2), fourth sentence, of the BSI Act of 14 August 2009 (BGBl. I, p. 2821), as last amended by Article 12 of the Act of 23 June 2021 (BGBl. I, p. 1982)’ through the words ‘Paragraph 2(39) of the BSI Law of… [insert: Date and reference of this Act]’.

Article 25

Amendment to Book V of the German Social Security Code, [Fünftes Buch Sozialgesetzbuch – SGB V]

Paragraph 103a of the Book Eleventh of the Social Code – Social Care Insurance – (Article 1 of the Act of 26 May 1994, BGBl. I p. 1014, 1015), most recently by Article 4 of the Act of 30 May 2024 (BGBl. 2024 I) No. 173) has been amended, is amended as follows:

1. IN paragraph 3 shall read the words: there shall be substituted: ‘Section 8a(2) of the BSI Act’‘Section 30(8) of the BSI Act’.

2. IN paragraph 5 shall read the words: ‘Critical infrastructure’ means: there shall be substituted: ‘critical installations’ means: and the words ‘Section 8a of the BSI Act’ in this regard, the Words ‘Section 30, 31 and 39 of the BSI Act’

Article 26

SIMILARnon-compliance with Telecommunications Act

The Telecommunications Act of 23 June 2021 (BGBl. I p. 1858), as last amended by Article 35 of the Act of 6 May 2024 (BGBl. 2024 I) No. 149)‘is amended as follows:

1. In the table of contents, the entry for Section 168 is worded as follows:

   Section 168: Incident notification’.

2. Section 3 is amended as follows:

   a) Subparagraph 53 is worded as follows:

      1. “Incident’ means an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered or accessible through network and information systems;’;.

   a) IN point 79 is replaced by a semicolon.

   b) Ethe following point 80 is added:

1. ‘Network and information system’

a) a telecommunications network as defined in point 65;

b) a device or a group of connected or related devices, one or more of which, on the basis of a programme, perform the automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by the elements referred to in points (a) and (b) for the purposes of their operation, use, protection and maintenance.’;

3. Section 165 is amended as follows:

a) Athe third sentence of the second paragraph is replaced by the following:

‘Those measures shall ensure a level of security of network and information systems appropriate to the risk involved, taking into account the state of the art, relevant European and international standards and the compliance costs. When assessing whether measures are proportionate to the risk involved, account shall be taken of the extent of the risk exposure and the size of the operator or provider, as well as the likelihood and severity of incidents, as well as their societal and economic impact.’;

b) Nin paragraph 2, the following paragraphs 2a to 2d are inserted:

‘(2a) Measures referred to in paragraph 2 by operators of public telecommunications networks and providers of publicly available telecommunications services which provide particularly important facilities within the meaning of: Section 28(1), first sentence, point 3 of the CBI Acts or important entities within the meaning of Section 28(2), first sentence, point 2 the BSI Act shall be based on an all-hazard approach aimed at protecting the network and information systems and the physical environment of these systems from incidents and shall include at least the following:

1. Approaches to risk evaluation and security for information systems;

2. Incident management,

3. Business continuity, such as backup management and post-emergency recovery, and crisis management;

4. Security of the supply chain, including security-related aspects of the relationship between each entity and its immediate suppliers or service providers;

5. Security measures for the acquisition, development and maintenance of network and information systems, including vulnerability management and disclosure;

6. Policies and procedures for assessing the effectiveness of measures referred to in paragraph 2 in the field of security of networks and services;

7. Basic procedures and training in the field of security of networks and services;

8. Policies and procedures for the use of cryptography and encryption;

9. Staff security, access control policies and facility management;

10. Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communication and, where appropriate, secured emergency communication systems within the facility.

(2b) The management of operators of public telecommunications networks and providers of publicly available telecommunications services which are particularly important facilities within the meaning of Section 28(1), first sentence, point 3, of the BSI Act or important facilities within the meaning of Section 28(2), first sentence, point 2, of the BSI Act shall be obliged to implement the measures to be taken by those entities pursuant to paragraph 2 and to monitor their implementation.

(2c) Business directors who fail to comply with their obligations under paragraph 2b shall be liable for any damage caused to their institution in accordance with the company law rules applicable to the legal form of the entity. Under that Act, they are liable only if the company law provisions governing the entity do not contain any liability regime under sentence 1.

2d The management of operators of public telecommunications networks and providers of publicly available telecommunications services, which are particularly important facilities within the meaning of Section 28(1), first sentence, point 3 of the BSI Act or important facilities within the meaning of Section 28(2), first sentence, point 2, of the BSI Act, shall regularly participate in training in order to acquire sufficient knowledge and skills to identify and assess risks and risk management practices in the field of information technology security and to be able to assess the impact of risks and risk management practices on the services provided by the entity.'

c) In the first sentence of paragraph 3, the indication: 'Section 2(9b) of the BSI Act' through the indication: 'Section 2(41) of the BSI Act'.

d) IN paragraph 4 is renumbered: 'Section 2(13) of the BSI Act' through the indication: 'Section 2(23) of the BSI Act'.

e) IN paragraph 11, first sentence, the indication 'Article 9 of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1); (OJ L 33, 7 February 2018, p. 5).' shall be replaced by 'Article 10 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14. December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).'.

4. Section 167 Paragraph 1, second sentence, subparagraph 1 is amended as follows:

a) The indication 'Section 2(13), first sentence, point 3(b) of the BSI Act' will shall be replaced by 'Section 2(23)(c)(bb) of the BSI Act'.

b) The indication 'Section 2(13) of the BSI Act' becomes das a result, the indication 'Section 2(23) of the BSI Act'.

5. Section 168 is amended as follows:

a) The heading is worded as follows:

§ 1‘

Incident notification’.

b) Paragraphs 1 to 3 are worded as follows:

(1) ‘ Any person operating a public telecommunications network or providing publicly available telecommunications services shall submit to the Federal Network Agency and the Federal Office for Information Security:

1. without undue delay and at the latest within 24 hours of becoming aware of a significant incident, an early initial notification indicating whether there is a suspicion that the significant incident is due to illegal or malicious acts or may have a cross-border impact;

2. without undue delay and at the latest within 72 hours of becoming aware of a significant incident, a notification of the incident confirming or updating the information referred to in point 1 and indicating an initial assessment of the significant incident, including its severity and impact, and, where applicable, the indicators of compromise;

3. at the request of the Federal Network Agency or the Federal Office for Security in Information Technology, an interim notification of relevant status updates;

4. No later than one month after the notification of the significant incident referred to in point 2, subject to paragraph 2, a closure report containing:

a) a detailed description of the significant incident, including its severity and impact;

b) The nature of the threat or underlying cause likely to have triggered the incident;

c) Information on the corrective measures taken and ongoing;

d) Where applicable, the cross-border impact of the significant incident.

Section 42 Paragraphs 4 and 43(4) of the Federal Data Protection Act shall apply accordingly.

(2) If the significant incident still persists at the time referred to in point (4) of paragraph 1, the person concerned shall submit a progress report and a closure notification at that time, instead of a final notification, within one month of the completion of the handling of the significant incident.

(3) An incident shall be considered to be significant if:

1. it has caused or is likely to cause serious operational disruptions or financial losses to the provider of public telecommunications networks or publicly available telecommunications services concerned; or

2. it has affected or is likely to affect other natural or legal persons by causing substantial material or non-material damage.’

c) IN paragraph 4 becomes the word: by the word: ‘Notification procedure’ means:‘Reporting procedure’ means:.

d) The following paragraph 5 is inserted after paragraph 4:

(1) ‘ The Federal Network Agency shall send an acknowledgement of receipt of the notification to the obliged entity pursuant to the first sentence of paragraph 1 without undue delay and, where possible, within 24 hours of the early initial notification referred to in point 1 of the first sentence of paragraph 1. The Federal Office for Information Security may, at the request of the obliged entities pursuant to the first sentence of paragraph 1, provide additional technical assistance, guidance or operational advice on remedial measures. The Federal Office for Information Security shall inform the Federal Network Agency of the measures referred to in the second sentence.’

e) The current paragraph (5) becomes paragraph (6) and is worded as follows:

(1) ‘ Where necessary, Bundesnetzagentur shall inform the national regulatory authorities of the other Member States of the European Union and the European Union Agency for Cybersecurity of the incident. Where public awareness is necessary to prevent or deal with a significant incident or if the disclosure of the significant incident is otherwise in the public interest, the Federal Network Agency may, after consulting the obliged entities pursuant to the first sentence of paragraph 1, inform the public or require obliged entities under the first sentence of paragraph 1 to provide such information.’

f) Dformer paragraph 6 becomes paragraph 7 and the indication: ‘Section 8e of the BSI Act’ if the indication: ‘Section 42 of the BSI Act’.

g) The previous paragraph (7) becomes paragraph (8).

6. IN Section 174(3)(8) and (5)(8) the words: ‘Areas covered by Section 2(10), first sentence, point 1, of the BSI Act’ there shall be substituted: ‘Sectors covered by Section 2(24) of the BSI Act’.

7. IN Section 214(3) shall read the words: ‘Critical Infrastructure’ means there shall be substituted: ‘critical installations’ means: and the indication: ‘Section 2(10) of the BSI Act’ through the indication: ‘Section 2(22) of the BSI Act’.

8. IN Section 228(2), point 39, the words: there shall be substituted: ‘a notification’‘a notification or notification’ means:.

Article 27

Amendment to the Hospital Structural Fund Ordinance

The Electronic Legal Correspondence Ordinance of 17 December 2015 (Federal Law Gazette (BGBl.) I p. 2350), last amended by Article 6 of the Act of 20 December 2022 (BGBl. I p. 2793), is amended as follows:

1. IN Section 11(1)(4)(a) shall be inserted after the words: the words ‘Part 3 of Annex 5 to the BSI Criti Regulation’‘of 22 April 2016 (BGBl. I p. 958), as last amended by Article 1 of the Ordinance of 29 November 2023 (BGBl. 2023 I) No. 339) has been amended,’; inserted and the words ‘to the requirements of Section 8a of the BSI Act’

there shall be substituted: ‘the requirements of Paragraphs 30, 31 and 39 of the BSI Act’.

2. IN Section 14(2)(8) shall read the words: ‘to the requirements of Section 8a of the BSI Act’ there shall be substituted: ‘the requirements of Paragraphs 30, 31 and 39 of the BSI Act’.

Article 28

Amendment to the Foreign Trade and Payments Ordinance

Section 55a(1) of the Foreign Trade Ordinance of 2 August 2013 (BGBl. I, p. 2865), as last amended by Article 3 of the Act of 27 February 2024 (BGBl. 2024 I) No. (71) has been amended;‘is amended as follows:

1. IN point 1 is renumbered the words: ‘Critical infrastructure’ means: there shall be substituted: ‘critical installation’ means:.

2. IN point 2 is renumbered the words: ‘Section 2(13) of the BSI Act’ through the words ‘Section 2(23) of the BSI Act’ and die words ‘Critical infrastructure’ means: there shall be substituted: ‘critical installations’ means:.

Article 29

Amendment to the Trust Services Act

Section 2 Paragraph 3 of the Trust Services Act of 18 July 2017 (BGBl. I p. 2745), as amended by Article 2 of the Act of 18 July 2017 (BGBl. I p. 2745)‘shall be repealed.

Article 30

Other amendments of the BSI Act

Das BSI Act, recast by Article 1 of this Act, is amended as follows:

1. Section 2 Point 22 is worded as follows:

   1. ‘‘Critical installation’ means an installation within the meaning of Section 2(3) of the umbrella law to strengthen the physical resilience of critical installations (KRITIS umbrella law);’.

2. Section 2 Point 24‘…’ Section 28 Paragraph 7 and Section 56(4) shall be repealed.

3. In Section 2(23) and Section 12 Paragraph 1, second sentence in each case, the information shall be: ‘Section 2(24)’ through the indication: ‘Section 4(1) of the KRITIS Common Law’.

4. In Section 33(2) and Section 41 Paragraph 2 sentence 1, paragraph 3 sentence 4, first sentence of paragraph 4, paragraph 6, 7 in each case, the information shall be:

‘Section 56(4)’ by DIE indication ‘Section 5(1) in conjunction with Section 4(3) of the KRITIS-Dachgesetz’.

5. IN Section 65(1), (2)(6) and (10) becomes dIE indication ‘Section 56(4), first sentence’ each shall be replaced by ‘Section 5(1) in conjunction with Section 4(3) of the KRITIS-Dachgesetz’.

Article 31

Wmore eiteration the Telecommunications Act

IN Section 174(3)(8) and (5)(8) of the Telecommunications Act of 23 June 2021 (BGBl. I p. 1858), as last amended by Article 26 this Law has been amended, the particulars of: ‘Section 2(24) of the BSI Act’ through the indication: ‘Section 4(1) of the KRITIS Common Law’.

Article 32

Additional amendments of the Foreign Trade Regulation

In Section 55a(1)(1) and (2) of the Foreign Trade Ordinance of 2 August 2013 (BGBl. I, p. 2865; 2021 I p. 4304), last amended by: Article 28 this Law has been amended, the indication: shall be replaced by ‘within the meaning of the BSI Act’‘pursuant to Section 2(3) of the KRITIS General Law’.

Article 33

Entry into force, expiry

(1) This law shall enter into force on the day following promulgation subject to paragraph 2. At the same time, the BSI Act of 14 August 2009 (BGBl. I, p. 2821) expires.

(2) The Articles 30, 31 and 32 enter into force on the date on which the statutory ordinance referred to in: Section 5(1) in conjunction with Section 4(3) the umbrella law on strengthening the physical resilience of critical installations (KRITIS umbrella law) enters into force, but not before the date of entry into force referred to in paragraph 1. The Federal Ministry of the Interior and Community shall announce the date of entry into force in the Federal Law Gazette.

Explanatory notes

A. General part

I. Objective of and need for the provisions

Germany’s modern economy depends on well-functioning and resilient infrastructure, both physical and digital, for its functioning, generating prosperity and growth, and also for its adaptability to changing economic policy and geopolitical framework conditions. These factors have significantly grown in importance in recent years. Companies face a variety of challenges not only in their economic activities, but also in their practical security. European-wide and globally interconnected processes, as well as the increasing digitalisation of all areas of life, and thus also of the economy, are leading to greater vulnerability to external, often non-controllable factors. Information technology plays a central role in critical installations as well as in certain companies. Their security and resilience form also the basis for security of supply, from the supply of electricity and water to the disposal of municipal waste. The same applies to the functioning of the market economy in Germany and the internal market of the European Union. The interconnectedness and close integration of the economy within Germany and the European Union is the result of interdependencies in cybersecurity. In this context, the increased cybersecurity requirements for legal and natural persons providing essential services or carrying out activities are set out in Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80; ‘NIS 2 Directive’) further aligned across the European Union.

The NIS 2 Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market. To this end, the NIS 2 Directive lays down obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs). It also lays down cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II of the NIS 2 Directive as well as for entities identified as critical entities under Directive (EU) 2022/2557. In addition, the NIS 2 Directive lays down rules and obligations on cybersecurity information sharing, as well as supervisory and enforcement obligations on Member States.

The requirements of the NIS 2 Directive are based on Article 114 TFEU and aim to harmonise the internal market of the European Union. In addition to the other considerations outlined in the preamble to the draft bill, the requirements are therefore implemented, in particular in order to eliminate and avoid distortions in the internal market. The cybersecurity requirements would otherwise differ considerably from one Member State to another. Such differences in cybersecurity requirements and supervision would create additional costs for economic operators and have a negative impact on the cross-border supply of goods or services.

In its 2023 report on the state of IT security in Germany, the Federal Office for Information Security (BSI) estimates that the overall IT security situation has worsened as a result of Russia's war of aggression against Ukraine, which violates international law. In the field of business, ransomware attacks, exploitation of vulnerabilities, open or incorrectly configured online servers as well as dependencies on the IT supply chain and, in this context, cyberattacks via the supply chain (so-called supply chain attacks) are among the greatest

threats. In addition to the already known threats, the Russia's war of aggression against Ukraine and the resulting ‘turning point’ also gave rise to new threats or the assessments of already known threats had to be changed due to changing framework conditions. Examples of this are in the field of hacktivism, in particular through distributed denial of service (DDoS) attacks or collateral damage caused in Germany as a result of cyber sabotage attacks in the context of the war. In addition, supply chain disruptions and attacks, both in the areas of cybercrime and war, have also increased recently. These phenomena are no longer occurring only occasionally, but have become part of everyday business life. Increasing the resilience of the economy to the dangers of the digital world is therefore a key task for the players involved in the state, economy and society in order to maintain Germany’s and the European Union’s internal market as a whole robust, efficient and functional as a business location.

For information security management in the federal administration, the previous governance tools have proven to be insufficiently effective on a predominantly sub-statutory basis to achieve a comprehensively effective increase in the level of security. This has been confirmed, in particular, by surveys on the current status of the Federal implementation plan and audits carried out by the Federal Court of Auditors (BRH). Against the backdrop of the current geopolitical developments (‘turning point’), the threat situation has once again intensified, further increasing the risk of governmental entities being restricted in their ability to act by threats from cyberspace.

In accordance with the requirements of EU law, the regulatory framework established by the Act on Increasing the Security of Information Technology Systems (IT Security Act) of 17 July 2015 (Federal Law Gazette (BGBl.) I 2015, p. 1324) and the Second Act on the Enhancement of the Security of Information Technology Systems (IT Security Act 2.0) of 18 May 2021 (Federal Law Gazette (BGBl.) I 2021, p. 1122) is extended to the area of certain undertakings by the NIS 2 Transposition and Cybersecurity Enhancement Act; in addition, corresponding requirements for the federal administration are introduced. Due to the large scope of the project, it is linked to an amendement of the BSI Act. In this context, the mandate from the coalition agreement for the 20th legislative period, line 438, to further develop IT security law is also taken up.

This draft is in the context of the efforts of the European Union and its Member States to increase economic security and enhance resilience in response to a new geopolitical framework conditions. With the European Economic Security Strategy, published on 20 June 2023, the European Commission identifies the risk to the security of critical infrastructure from physical and cyberattacks as one of four main risks for the European economy.

This draft is also in the context of the jeopardised timely achievement of the goals of the United Nations General Assembly resolution of 25 September 2015 entitled ‘Transforming our world: the UN 2030 Agenda for Sustainable Development’. In particular, the draft aims to contribute to the achievement of Sustainable Development Goal 9 of the UN 2030 Agenda to build high-quality, reliable and resilient infrastructure.

II. Main content of the draft

The requirements of European Union law of the NIS 2 Directive are being implemented as part of an amendment to the Act on the Federal Office for Information Security (BSI Act) and individual specialist laws. In addition, the information security management in the federal administration is being strengthened. The new rules on the companies covered by the scope are aimed in particular at strengthening the resilience of the economy, which has become necessary in the light of the increased cyber threat situation and the implications of the ‘turning point’. In detail:

– Introducing the defined categories of particularly important and important entities, providing for a significant extension of the scope so far limited to critical infrastructure operators, digital service providers and businesses in the particular public interest.

– Maintaining the KRITIS entity category as an additional category for companies requiring special protection, with corresponding requirements.

– The catalogue of minimum security requirements of Article 21(2) of the NIS 2 Directive is incorporated into the BSI Act, distinguishing between categories in the intensity of the measure in question for reasons of proportionality.

– Legally enshrining essential national requirements for federal information security management and mapping the associated roles and responsibilities.

– Harmonising requirements for Federal Administration entities arising from national and EU legislation in order to ensure a coherent and manageable regulatory regime overall.

– Introducing a three-step reporting regime that minimises the bureaucratic burden on entities within the scope of implementation and explores and exploits possible synergies with further reporting obligations, in particular to monitor disruptions of the planned umbrella law on strengthening the physical resilience of critical facilities (KRITIS umbrella law).

– Complementing BSI's supervisory tools: it implements a fine framework in line with the EU General Data Protection Regulation, which distinguishes between KRITIS and particularly important entities, on the one hand, and important entities on the other.

– Implementing an exclusion clause for companies with a specific link to the security and defence sector. The relevant security/defence requirements then apply to such entities.

– Establishing a federal CISO as the central coordinator for information security measures in Federal Administration entities and to assist the departments in implementing the information security management requirements.

– Further developing the BSI CritisV so that entities below the size-cap rule, for which the NIS 2 Directive provides for identification on the basis of criticality criteria as a special case, can be recorded.

III. Alternatives

None.

IV. Legislative powers

For the amendment to the BSI Act in Article 1the amendment to the BSI Act in Article 30the amendment to the IT Security Act 2.0 in Article 7the amendment to the EnWG in Article 17, the amendment to the Energy Security Act in Article 19 and the amendment to the Telecommunications Act in Article 26, which concern the purely technical protection of information technology of and for critical facilities and particularly important entities and important entities, the legislative competence of the Federal Government follows from Article 73(1)(7) (telecommunications) of the Basic Law (GG) and from Article 74(1)(11) of the Basic Law (Law of the economy, including ancillary competence under security law) in conjunction with Article 72(2) of the Basic Law and Article 74(1)(12) of the Basic Law (social security, including unemployment insurance).

A regulation of this matter under federal laws is required in the overall interest of the state in order to maintain the economic unit in the federal territory. A regulation by the legislator of a Land would result in significant disadvantages for the overall economy which cannot be accepted, neither in the interests of the Federal Government nor the Länder. In particular, it would have to be feared that different treatments under federal state law of the same circumstances of life, for example different prerequisites for issuing security certificates, would result in a significant distortion of competition and disturbing barriers for economic activities within Länder. International agreements on the mutual recognition of IT security certificates and the exchange through a single point of contact pursuant to Article 8(3) of the NIS 2 Directive require federal legislation. The conditions set out in Article 72(2) of the Basic Law are also met with regard to the new rules for KRITIS operators. Operators of critical facilities, as well as particularly important entities and important entities, represent essential parts of the economy in Germany, whose level of cybersecurity must be raised in the context of the increased threat situation (‘turning point’). Raising the level of cybersecurity of essential parts of the economy in Germany in the form of a federal law regulation is also necessary in order to maintain economic unity in the federal territory in the interest of the State. Regional differences in companies’ level of cybersecurity would lead to significant distortions of competition and disruptive barriers to economic activity within Länder.

For regulations in Articles 1 and 30 on the protection of the federal administration, the Federation has legislative competence by virtue of the nature of the matter.

With a view to the Federation’s overall responsibility, the Federal Government’s competence for regulations on nationwide notifications, including any recommendations and warnings to consumers in the field of information security also follows from the very nature of the matter (government leadership) because issues relating to IT security regularly have supraregional effects in view of the ever-increasing digitisation and networking of all areas of life.

The Federal Government also has exclusive legislative competence under Article 73(1)(8) of the Basic Law for the legal relationships of persons in the service of the Federal Government and of public corporations that the Federal Government indirectly owns.

The legislative competence of the Federal Government for the provisions on fines and administrative offences in Article 1 follows from Article 74(1)(1) of the Basic Law (criminal law).

The legislative competence of the Federal Government to amend the Sixth Book of the Social Security Code in Article 23 arises from Article 74(1)(12) of the Basic Law.

The Federal Government’s legislative competences for the consequential amendments to the BSI Act are the same as for Article 1.

V. Compatibility with European Union law and international treaties

The draft Act is compatible with the Law of the European Union. It largely supports the implementation of the NIS 2 Directive, amending the BSI Act (Article 1) in detail:

– Maintaining the identification of critical facilities (formerly critical infrastructure) and regulating their operators maintains an existing regime that is not covered by the NIS 2 Directive.

– The categories of essential and important entities defined by the NIS 2 Directive will be implemented with the newly introduced categories of entities of particularly important and important entities.

– The regulation of federal administration entities (Part 2, Chapter 3) is a set of rules implementing the NIS 2 Directive insofar as an entity of the federal administration is part of the central government within the meaning of Article 2(2)(f)(i) of the NIS 2 Directive. For the purposes of implementing the NIS 2 Directive, the term ‘central government’ in Germany within the meaning of the NIS 2 Directive – in line with the German definition of ‘central government authorities’ in Directive 2014/24/EU – generally refers to federal ministries and the Federal Chancellery, each without any subordinate area. In addition, these are regulations that deviate from the regulations for (particularly) important entities for federal administration institutions, as well as existing rules under the BSI Act and supplementary national rules.

The draft Act is compatible with the international agreements concluded by the Federal Republic of Germany.

VI. Impact of the Act

1. Legislative and administrative simplification

The draft Act contributes to legal simplification by amending the existing BSI Act. The BSI Act will be reorganised and restructured, making the work of legal practitioners easier. Furthermore, the draft Act contributes to administrative simplification by sharpening the rights and obligations of the Federal Office, in particular vis-à-vis other supervisory authorities, and thus further specifying responsibilities. The aim of a common reporting portal with other supervisory authorities is to exploit synergies in the reporting obligations of the operators and entities covered and to minimise red tape. Finally, the legal incorporation of existing sub-statutory rules on information security management will further strengthen the IT security of the federal public administration.

2. Sustainability aspects

The draft Act is in line with the Federal Government’s guiding principle on sustainable development within the meaning of the German Sustainable Development Strategy, which serves to implement the UN 2030 Agenda for Sustainable Development. By largely implementing the NIS 2 Directive, which regulates the necessary cybersecurity requirements for legal and natural persons providing essential services or activities, the draft contributes to the achievement of SDG 9 ‘Build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation’. Target 9.1 of this Sustainable Development Goal requires high-quality, reliable, sustainable and resilient infrastructure, including regional and cross-border infrastructure, to support economic development and human well-being. The draft promotes the achievement of this target by improving the security of information technology in critical facilities, in particular for the supply of vital water and energy to the population.

At the same time, in the spirit of the systemic understanding of the SDGs, the draft contributes to the achievement of Goal 16, which requires in its Target 16.6 to develop effective, accountable and transparent institutions at all levels. The draft promotes the achievement of this target, in particular by strengthening information security management in the federal administration and strengthening the importance of the Federal Office for Information Security.

The draft thus also contributes to the achievement of further Sustainable Development Goals (SDGs) of the UN 2030 Agenda:

Goal 3. ‘Ensure healthy lives for all at all ages and promote their well-being’ by strengthening the quality of life through the creation of a high level of cyber security and ensuring security of supply for citizens;

Goal 8. ‘Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all’; and

Goal 11. ‘Make cities and human settlements inclusive, safe, resilient and sustainable’.

The draft thus takes into account the interconnections between the SDGs and their integrating nature, which is crucial for the achievement of the objective and purpose of the UN 2030 Agenda. The draft follows the sustainability principles of the German Sustainability Strategy (Deutsche Nachhaltigkeitsstrategie, DNS) ‘(1.) Apply sustainable development as a guiding principle at all times and in all decisions’, ‘(2.) Assume global responsibility’, ‘(4.) Strengthen sustainable economic activity’, ‘(5.) Preserve and enhance social cohesion in an open society’.

3. Budgetary expenditure exclusive of compliance costs

a. Overall statement

No additional budgetary expenditure, excluding compliance costs, is expected for the Länder and municipalities as a result of the Act. The additional budgetary expenditure, excluding compliance costs, for the Federal Government as a whole as a result of the Act is as follows.

Overall statement of federal budgetary expenditure:

	Budgetary expenditure in EUR thousand			
Budgetary year	**2026**	**2027**	**2028**	**2029**
Total per budgetary year	192,364	192,161	209,735	216,289
Cumulative amount in the budget period	810,549			

Overall statement of federal posts and positions:

	Posts and positions			
Budgetary year	**2026**	**2027**	**2028**	**2029**
Higher Service [hD]	218.37	303.96	388.07	418.67
Senior Service [gD]	365.95	439.9	496.4	515.2
Intermediate service [mD]	56.13	81.63	93.43	100.33
Cumulative amount of posts and positions in the budget period	1,034.2			

Overall statement of budgetary expenditure, social security institutions:

Budgetary expenditure	Budgetary expenditure in EUR thousand per budgetary year				Cumulative amount in EUR thousand in the budget period
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
Social security institutions	2,482	2,482	2,482	2,482	9,928
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	2,482	2,482	2,482	2,482	9,928

b. Budgetary expenditure by section including business plans

The total udgetary expenditure referred to under A.VI.3.a. is allocated to sections as follows:

Budgetary expenditure	Budgetary expenditure in EUR thousand per budgetary year				Cumulative amount in EUR thousand in the budget period
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
Overall presentation					
04 (Federal Chancellery, Press and Information Office of the Federal Government and Federal Government Commissioner for Culture and the Media)					
06 (Federal Ministry of the Interior and Community)	84,569.122	85,556.655	105,706.849	112,197.524	388,030.15
of which one-off expenditure:	23,986.8	0	0	0	23,986.8
of which annual expenditure:	60,582.342	85,556.655	105,706.849	112,197.524	360,043.370
09 (Federal Ministry of Economic Affairs and Climate Action)	14,231	9,489	9,363	9,426.3	42,509.3
of which one-off expenditure:	6,782	294	29	19.76	7,124.76
of which annual expenditure:	7,449	9,195	9,334	9,406.54	35,384.5
08 (Federal Ministry of Finance)	1,934	3,408	2,608	2,608	10,558
of which one-off expenditure:	900	0	0	0	900

Budgetary expenditure	**Budgetary expenditure in EUR thousand per budgetary year**				**Cumulative amount in EUR thousand in the budget period**
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
of which annual expenditure:	1,034	3,408	2,608	2,608	9,658
05 (Federal Foreign Office)	10,714	15,594	14,828	14,828	55,964
of which one-off expenditure:	1,791	766	0	0	2557
of which annual expenditure:	8,923	14,828	14,828	14,828	53,407
07 (Federal Ministry of Justice)	5,067	2,496	2,496	2,496	12,555
of which one-off expenditure:	2,571	0	0	0	2,571
of which annual expenditure:	2,496	2,496	2,496	2,496	9,984
11 (Federal Ministry of Labour and Social Affairs)	5,232	5,232	5,232	5,232	20,928
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	5,232	5,232	5,232	5,232	20,928
14 (Federal Ministry of Defence)	0	0	0	0	0
10 (Federal Ministry of Food and Agriculture)	2,127	1,572	1,521	1,521	6,741
of which one-off expenditure:	605.5	56	0	0	661.5
of which annual expenditure:	1521	1,521	1,521	1,521	6,084
17 (Federal Ministry of Family Affairs, Senior Citizens, Women and Youth)	2,240	2,180	2,180	2,180	8,780
of which one-off expenditure:	60	0	0	0	60
of which annual expenditure:	2,180	2,180	2,180	2,180	8,720
15 (Federal Ministry of Health)	6,864	6,864	6,864	6,864	27,456

Budgetary expenditure	**Budgetary expenditure in EUR thousand per budgetary year**				**Cumulative amount in EUR thousand in the budget period**
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	6,864	6,864	6,864	6,864	27,456
12 (Federal Ministry of Digital and Transport)	2,257	2,140	1,620	1,620	7,637
of which one-off expenditure:	174.2	57.5	58	58	347.7
of which annual expenditure:	2,082	2,082	1,562	1,562	7,288.8
16 (Federal Ministry of the Environment, Nature Conservation, Nuclear Safety and Consumer Protection)	5,469	5,136	5,136	5,136	20,877
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	5,469	5,136	5,136	5,136	20,877
30 (Federal Ministry of Education and Research)	85	53	53	53	244
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	85	53	53	53	244
23 (Federal Ministry of Economic Cooperation and Development)	2,008	3,709	3,401	3,401	12,519
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	2,008	3,709	3,401	3,401	12,519
25 (Federal Ministry of Housing, Urban Development and Construction)	1,355	495	495	495	2,840
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	1,355	495	495	495	2,840

Budgetary expenditure	Budgetary expenditure in EUR thousand per budgetary year				Cumulative amount in EUR thousand in the budget period
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
21 (Federal Commissioner for Data Protection and Freedom of Information)	1,140	1,140	1,140	1,140	4,560
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	1,140	1,140	1,140	1,140	1,140

c. Positions and posts by section

The positions and posts in the overall list of positions and posts referred to in A.VI.3.a. are allocated to the sections as follows:

Posts and positions					
Section	**Budgetary year**	**2026**	**2027**	**2028**	**2029**
Overall presentation **04** (Federal Chancellery, Press and Information Office of the Federal Government and Federal Government Commissioner for Culture and the Media) **06** (Federal Ministry of the Interior and Community)	697.69 Posts/positions	313.19	491.99	641.79	697.69
	Higher Service	121.42	212.42	295.42	325.42
	Senior Service	160.75	223.25	278.25	297.25
	Intermediate service	31.02	56.32	68.12	75.02
09 (Federal Ministry of Economic Affairs and Climate Action)	56.32 Posts/positions	48.6	55.31	55.92	56.32
	Higher Service	12.8	15.39	15.5	16.1
	Senior Service	31.5	35.4	35.9	35.7
	Intermediate service	4.32	4.52	4.52	4.52
08 (Federal Ministry of Finance)	7 Posts/positions	4	7	7	7
	Higher Service	0	1	1	1

Posts and positions					
Section	**Budgetary year**	**2026**	**2027**	**2028**	**2029**
	Senior Service	3	5	5	5
	Intermediate service	1	1	1	1
05 (Federal Foreign Office)	95.8 Posts/positions	95.8	95.8	95.8	95.8
	Higher Service	23.7	23.7	23.7	23.7
	Senior Service	68.9	68.9	68.9	68.9
	Intermediate service	3.21	3.21	3.21	3.21
07 (Federal Ministry of Justice)	30 Posts/positions	30	18	18	18
	Higher Service	14	5	5	5
	Senior Service	11.5	9	9	9
	Intermediate service	4.5	4	4	4
11 (Federal Ministry of Labour and Social Affairs)	27 Posts/positions	27	27	27	27
	Higher Service	6.5	6.5	6.5	6.5
	Senior Service	20.5	20.5	20.5	20.5
	Intermediate service	0	0	0	0
14 (Federal Ministry of Defence)	0 Posts/positions	0	0	0	0
	Higher Service	0	0	0	0
	Senior Service	0	0	0	0
	Intermediate service	0	0	0	0
10 (Federal Ministry of Food and Agriculture)	8.98 Posts/positions	8.73	8.98	8.98	8.98
	Higher Service	2.43	2.5	2.5	2.5
	Senior Service	6.3	6.48	6.48	6.48
	Intermediate service	0	0	0	0

Posts and positions					
Section	**Budgetary year**	**2026**	**2027**	**2028**	**2029**
17 (Federal Ministry of Family Affairs, Senior Citizens, Women and Youth)	13.2 Posts/positions	13.2	13.2	13.25	13.25
	Higher Service	7.2	7.2	7.2	7.2
	Senior Service	5.75	5.75	5.75	5.75
	Intermediate service	0.25	0.25	0.25	0.25
15 (Federal Ministry of Health)	23.3 Posts/positions	23.3	23.3	23.3	23.3
	Higher Service	9.1	9.1	9.1	9.1
	Senior Service	11.2	11.2	11.2	11.2
	Intermediate service	3	3	3	3
12 (Federal Ministry of Digital and Transport)	35.8 Posts/positions	35.8	35.8	35.8	35.8
	Higher Service	6.9	6.9	6.9	6.9
	Senior Service	25.12	25.12	25.12	25.12
	Intermediate service	3.8	3.8	3.8	3.8
16 (Federal Ministry of the Environment, Nature Conservation, Nuclear Safety and Consumer Protection)	28.35 Posts/positions	19.63	28.35	28.35	28.35
	Higher Service	6.42	8.25	8.25	8.25
	Senior Service	12.21	18.6	18.6	18.6
	Intermediate service	1	1.5	1.5	1.5
30 (Federal Ministry of Education and Research)	0.54 Posts/positions	0.54	0.16	0.16	0.16
	Higher Service	0	0	0	0
	Senior Service	0.54	0.16	0.16	0.16
	Intermediate service	0	0	0	0
23 (Federal Ministry of Eco-	12 Posts/posi-	9	10	12	12

Posts and positions					
Section	**Budgetary year**	**2026**	**2027**	**2028**	**2029**
nomic Cooperation and Development)	tions				
	Higher Service	2	2	3	3
	Senior Service	3	4	5	5
	Intermediate service	4	4	4	4
25 (Federal Ministry of Housing, Urban Development and Construction)	5.6 Posts/positions	5.6	5	5	5
	Higher Service	2.9	1	1	1
	Senior Service	2.7	4	4	4
	Intermediate service	0	0	0	0
21 (Federal Commissioner for Data Protection and Freedom of Information)	6 Posts/positions	6	6	6	6
	Higher Service	3	3	3	3
	Senior Service	3	3	3	3
	Intermediate service	0	0	0	0

The need for material and personnel resources as well as positions and posts should be balanced financially and in terms of posts in the relevant section of the budget. This also applies to the compliance costs presented under A.IV.4.c, insofar as these have an impact on the budget.

d. Impact on social security institutions

Budgetary expenditure	**Budgetary expenditure in EUR thousand per budgetary year**				**Cumulative amount in EUR thousand in the budget period**
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
Social security institutions	4,142	4,142	4,142	4,142	16,568
of which one-off expenditure:	0	0	0	0	0
of which annual expenditure:	4,142	4,142	4,142	4,142	16,568
Federal Employment Agency	1,517	1,517	1,517	1,517	6,068

Budgetary expenditure	Budgetary expenditure in EUR thousand per budgetary year				Cumulative amount in EUR thousand in the budget period
EPL / Budgetary year	**2026**	**2027**	**2028**	**2029**	
Social Insurance for Agriculture, Forestry and Horticulture (SVLFG)	940	940	940	940	3760
Deutsche Post Pension Service	25	25	25	25	100
Federal pension insurance institution (DRV)	1,660	1,660	1,660	1,660	6,640

Posts and positions					
	Budgetary year	**2026**	**2027**	**2028**	**2029**
Social security institutions	31.35 Posts	31.35	31.35	31.35	31.35
Federal Employment Agency	Higher Service	2	2	2	2
Social Insurance for Agriculture, Forestry and Horticulture (SVLFG)		0	0	0	0
Deutsche Post Pension Service		0	0	0	0
Federal pension insurance institution (DRV)		5	5	5	5
Federal Employment Agency	Senior Service	5	5	5	5
Social Insurance for Agriculture, Forestry and Horticulture (SVLFG)		2	2	2	2
Deutsche Post Pension Service		0.35	0.35	0.35	0.35
Federal pension insurance institution (DRV)		17	17	17	17
Federal Employment Agency	Intermediate service	0	0	0	0
Social Insurance for Agriculture, Forestry and Horticulture (SVLFG)		0	0	0	0
Deutsche Post Pension Service		0	0	0	0
Federal pension insurance institution (DRV)		0	0	0	0

4. Compliance costs

a. Compliance costs for citizens

Citizens will not incur any implementing costs.

b. Compliance costs for businesses

For businesses, annual compliance costs will rise by around EUR 2.2 billion. In total, one-off expenditure of around EUR 2.1 billion will be incurred. This is almost exclusively assigned to this category

Introduction or adaptation of digital process flows

.

Of this, approximately EUR 1.9 million is spent on administrative costs resulting from information obligations.

The burdens are not to be compensated under the One in, one out rule of the Federal Government, as these amendments result from a 1:1 transposition of the mandatory minimum requirements of Directive (EU) 2022/2555.

aa. Substantial legislative amendment

Requirement 4.2.1 (further requirement): Compliance with a minimum level of IT security (particularly important and important entities); Sections 30, 31 and 38(1) in conjunction with Section 28 BSIG-E, Section 5c(1) and (2) EnWG-E, Section 165(2) and (2a) TKG

Change in annual compliance costs:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
2,950	2,752	52.30	60,000	424,592	177,000
17,900	1,100	52.30	24,000	1,029,787	429,600
Change in compliance costs (in EUR thousand)				2,060,979	

One-off compliance costs: 2.1 EUR billion

Operators of critical facilities and providers of digital services are already obliged to ensure a minimum level of IT security (cf. Section 8a and 8c BSIG, Section 11(1a) et seq. EnWG and Section 165 TKG). The draft regulation continues to apply standards comparable to Sections 30, 31 and 38(1) in conjunction with Section 28 BSIG-E and Section 5c(1) and (2) EnWG and Section 165(2) and (2a) TKG, the scope of which will significantly increase the number of undertakings. In future, all particularly important and important entities should take appropriate, proportionate and effective technical and organisational measures to avoid IT-related disruptions relevant to their service provision (Section 30(1) BSIG-E). With regard to proportionality, the explanatory memorandum to Section 30 BSIG-E, Section 5c(3) EnWG-E or Section 165(2) TKG-E refers to the assessment criteria of established IT standards, compliance costs and existing risks. The latter are determined by the risk exposure, the size of the entity or operator, as well as the likelihood and severity of security incidents, as well as their societal and economic impact. As a result, necessary risk management measures that need to be taken by particularly important entities will be more extensive than those that essential entities will have to take. Managers are obliged to approve and monitor the risk measures (cf. Section 38(1) BSIG-E).

On the basis of information provided by the BMWK and data from the Federal Statistical Office's (StBA) business register, it can be assumed that in Germany in future around 8,250 companies are to be classified as particularly important and some 21,600 as important entities attributable to the addressee of legal norm – including municipal or state-owned enterprises and legal persons under public law which do not operate in the ‘public

administration' sector (cf. Directive (EU) 2022/2555 of the European Parliament and of the Council, Annex 1). Among the particularly important entities, there are 4,693 providers of digital services and operators of critical facilities, which already have to implement measures under current legislation (see online database of the compliance costs of the StBA (Ondea), ID 2015030909595401, 2017052913283301, 2020093009264301 und 2020093009264401). As a result, the legislative amendment only creates completely new legal obligations for the remaining 3,550 particularly important entities – and for the important entities. It should be noted that some of these potentially affected companies are already taking the required security measures. According to a study, 17 % of companies surveyed considered themselves very well against cyberattacks in 2023 (cf. eco – Verband der Internetwirtschaft e.V. (2023): https://www.eco.de/presse/eco-it-sicherheitsumfrage-2023-viele-unternehmen-unterschaetzen-noch-immer-bedrohungslage/ In the absence of other data, it is assumed on the basis of this study that around 17 % of the companies concerned are already taking sufficient measures in line of the transposing law. Consequently, the following calculation assumes that around 2,950 (= 0.83 * 3,550) particularly important entities and around 17,900 (= 0.83 * 21,600) important entities will incur implementing costs.

For company-related personnel and material costs, data from the Federal Statistical Office (StBA) are used, which were obtained by means of a survey of operators of critical infrastructure at the end of 2020 as part of the re-measurement of the implementing costs of the Act on Increasing the Security of Information Technology Systems and the Act transposing Directive (EU) 2016/1148. Thus, the additional personnel costs of critical infrastructure operators to comply with a minimum level of IT security resulting from these laws amount to an average of 2,752 hours and EUR 60,000 in material costs (see OnDEA, ID 2015030909595401 and 2017052913283301). With a view to implementing proportionate measures, this burden is also assumed for the particularly important entities concerned. In line with the proportionality assessment criteria, important entities face a reduced burden. In the absence of available data, it is assumed that this effort is, on average, 60 % lower, i.e. staffing of around 1,100 hours and material costs of EUR 24,000. Since it can be estimated, on the basis of the data from the BMWK and the StBA, that 13 % of the important entities are accounted for by large enterprises and 87 % for medium-sized enterprises, the average cost of 1,100 hours and EUR 24,000 corresponds to a situation in which the costs of large important entities correspond to 70 % of the costs of particularly important entities and that of medium-sized important entities to 35 % of the costs of the particularly important facilities.

If the parameters set out above are applied, an average wage rate of 52.30 per hour can be applied (cf. guidance document on the determination and presentation of compliance costs (hereafter: Guidance document), Section 7, Economy A-S excluding O; medium qualification level at 25 per cent, high qualification level at 75 per cent; and OnDEA ID 2015030909595401 and 2017052913283301) estimate the annual compliance costs of some EUR 600 million and EUR 1.5 billion respectively for particularly important entities and important entities.

With regard to the one-off expediture, there are no indications for an estimate. It is simplisticly assumed that the implementation of new IT infrastructure or the adaptation of the existing IT infrastructure to meet the required minimum level of IT security will involve an additional one-off expenditure corresponding to the annual expenditure for one year. The extensive survey of the federal administration revealed a similar ratio between the annual and the one-off expenditure (cf. requirement 4.3.1). As a result, a one-off compliance expenditure of the cost category 'Introduction and adaptation of digital processes' is expected to amount to almost EUR 2.1 billion.

As the draft regulation transposes Directive (EU) 2022/2555 of the European Parliament and of the Council, the national design to enhance the security of information technology systems is strictly limited. The objective of the 'concept to increase transparency on the

transition burden for the economy and to limit it effectively and proportionately' is therefore taken into account, as the transposing Act does not go beyond the regulatory content of the Directive. However, even when the EU Directive was being drafted, the Federal Government has also successfully promoted less costly solutions in the trilogue negotiations in line with the concept. Unlike the current Directive, the European Commission's proposal for a directive did not provide for differentiated rules for particularly important and important entities. Within the meaning of Article 21 and recital 15, the transposing Act now sets out the proportionality approach with regard to the measures to be taken, thereby placing a less monetary burden on important entities than the particularly important ones. The EU Commission's proposal also envisaged that if there is sufficient public participation in an entity, it would also fall within the scope of application if it is a small or micro-enterprise. As the criterion of public participation is no longer relevant, they are no longer in scope (with a few exceptions due to the details in Article 2). Finally, compared to the proposal for a Directive, the current EU Directive has narrowed the scope of application in some sectors, in particular for food businesses.

Specification 4.2.2 (Reporting obligation): Security incidents (reporting, notification and information obligations); Sections 32, 35 and 40(5) in conjunction with Section 28 BSIG-E, Section 5c(6) and (7) EnWG-E, Section 168(1) to (3) TKG-E

Change in annual compliance costs:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
2,400	6.75	58.40	0	946	0
450	2.25	58.40	0	59	0
2,85	1.00	58.40	0	17	0
Change in compliance costs (in EUR thousand)				1,022	

In the context of security incidents, the draft regulation provides for reporting obligations for particularly important and important entities vis-à-vis a reporting body, in certain cases an obligation to provide information and, on request, an obligation to provide information (cf. Sections 32, 35 and 40(5) BSIG-E, Section 5c(6) and (7) EnWG-E, Section 168(1) to (3) TKG-E). Already today, operators of critical infrastructure (cf. Section 8b(4) BSIG, Section 44b AtG), undertakings in the particular public interest (cf. Section 8f(7) and (8) BSIG), digital service providers (cf. Section 8c(3) BSIG) and undertakings in the telecommunications and energy sectors (cf. Section 11(1c) EnWG, Section 168 TKG) already have to report security incidents. Compliance costs arise as (a) more undertakings will be required to report and provide information, (b) the reporting obligation itself becomes more burdensome also for undertakings already subject to reporting obligations as a result of the future multi-stage procedure, and (c) the obligation to notify will be introduced.

The number of reported security incidents in the 2021/2022 reporting year was around 450 (cf. BSI, 2022 The Situation of IT Security in Germany, p. 68, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8). Assuming a similar amount of reporting for the new 25,157 (= 29,850 - 4,693) reporting companies per year, an additional 2,400 reported security incidents are expected.

The time spent on a case-by-case basis is around 4.5 hours for reporting under the current legal situation (see OnDEA, ID 2017052913283701 and 2015030909595201). As a result of the multi-stage reporting procedure, a surcharge of 50 per cent is simplified, with the result that a total duration of 6.75 hours per security incident or 16,200 hours (= 6.75*2,400) is assumed for the new reporting entities as a whole. For the companies currently required to report, the time spent is increased by 2.25 hours per report, or together

around 1,000 additional hours. For the obligation to provide information, it is simplified to assume that in no more than 10 % of all about 2,850 security incidents reported an additional time of around one hour, i.e. a maximum of 285 hours together.

With a total time spent of around 17,500 hours and a wage rate of EUR 58.40 per hour (see the Guidance document, Annex 7, economy as a whole (A-S excluding O), high skill levels), the total annual compliance costs amount to around one million euros.

Specification 4.2.3 (Reporting obligation): Registration obligations for particularly important and important entities and certain types of entities; Sections 33 and 34 in conjunction with Section 28 BSIG-E, Section 5c(8) EnWG-E

Change in annual compliance costs: 48,000 EUR

One-off compliance costs: 361,000 EUR

The draft regulation extends the existing registration requirement (cf. Sections 8b and 8f BSIG) to all particularly important and important entities and for certain types of entities. The first submission of the information gives rise to one-off compliance costs. Annual compliance costs arise from the obligation to notify changes to the information subject to the register (cf. Sections 33 and 34 in conjunction with Section 28 BSIG-E and Section 5c(8) EnWG).

Assuming that a total of around 6,000 operators of critical infrastructure and undertakings in the particular public interest are already registered today, an additional 23,850 particularly important and important entities in Germany will come under the scope of the legislative amendments. A one-off time of 25 minutes (standard activities 1, 2 and 3 of medium complexity and 5, 7 and 8 in simple complexity) is assumed for the initial compilation and transmission of the information in accordance with Annex 5 of the Guidance document. At a wage rate of EUR 36.30 per hour (see Guidance document, Annex 7, Total Economy A-S excluding O; medium level of qualification) incurs one-off compliance costs for the category of one-off information of approximately EUR 361,000. Assuming that the BSI implements an electronic registration procedure, there will be no further material costs arising from the transmission of data.

The (particularly) important entities must inform the competent authority of any changes (cf. Sections 33(5) and 34(2) BSIG-E). One third of the entities is expected to change at least one figure per year (= around 7,950 cases). With a case-related time of 10 minutes (see the Guidance document, Annex 5, standard activities 2, 3, 5, 7 and 8 in simple complexity) and a pay rate of EUR 36.30 per hour, the annual compliance costs amount to approximately EUR 48,000.

Requirement 4.2.4 (further requirement): Regular training (particularly important and important entities); Section 38 (3) in conjunction with Section 28 BSIG-E

Change in annual compliance costs:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
150,000	4	58.40	100	35,040	15,000
3,000,000	1	36.30	0	108,900	
Change in compliance costs (in EUR thousand)				158,940	

The draft regulation stipulates that managers of all addressed entities must regularly complete cyber security training; the other staff should attend such training on a regular basis (cf. Section 38(3) BISG-E).

The tImplementation Act (see explanatory memorandum) and the NIS 2 Directive (cf. Article 20(2)) only make general requests for training to acquire general knowledge and skills to identify and assess, inter alia, cybersecurity risks. Although the training is to be followed regularly, no specific periodicity is specified. In addition, it is unclear who is actually one of the business managers in the company. Finally, it is not clear what level of specialised cybersecurity training needs to be. Theoretically, these can be short training courses lasting a few hours, or seminars lasting several days due to the complexity of the subject matter.

It is estimated that around 298,500 business managers follow training courses per year. This is based on the free assumption that, once a year, ten managers per company will participate in such training (29,850 companies * 10). However, it can be assumed that some companies are already offering cyber security training to their leading employees out of their own interest. It is therefore assumed that this applies to 50 per cent of companies, meaning that it can be assumed that the status quo will change for around 150,000 managerial employees.

Furthermore, it is freely assumed that the training is on average half a day (4 hours). At a wage rate of EUR 58.40 per hour (see the Guidance document, Annex 7, economy as a whole (A-S excluding O), high skill levels), annual staff costs amount to almost EUR 35 million. If additional training costs for training provided by external lecturers of EUR 100 per participant are assumed, an additional annual material cost of EUR 15 million will be incurred. It should be noted that there are already free online trainings on IT security. If these were sufficient to meet the legal requirements for business managers, the material costs would be significantly lower.

As regards the training of staff, it is assumed that training will be provided to all or most of the persons employed in the entities classified as particularly important and important. On the basis of data from the StBA, it was calculated that the average number of employees in large and medium-sized enterprises is above 200. It is simplified to assume that each of the approximately 29,850 entities will complete cybersecurity training on average 200 employees. As with business managers, it is estimated that around 50 per cent of companies already allow their employees to take part in relevant cybersecurity training, leading to around three million people to be trained. It is also assumed that the training courses are less time-consuming than those completed by members of the governing bodies. In this scenario, it is assumed that an average of one one-hour training course or self-study unit is completed per year and that the majority of free offers that already exist today are used (cf. BSI, IT basic protection training, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html). Under the above assumptions, a wage rate of EUR 36.30 per hour (wage costs of total economy A-S excluding O; average skill level) trdults in an additional annual compliance costs of around 109 million euro.

Overall, the annual compliance costs for training managers and staff members amount to around EUR 159 million.

Requirement 4.2.5 (information obligation): Proof of compliance with IT security requirements (particularly important and important entities); Section 61 (3), (4) and (62) in conjunction with Section 28 BSIG-E

Change in annual compliance costs:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
24	282	56.94	19,300	385	463
Change in compliance costs (in EUR thousand)				849	

The BSI may request evidence of compliance with IT security requirements from a selection of particularly important entities. It should use certain criteria, such as the extent of the risk exposure, in order to identify entities subject to proof (cf. Section 64(3) and (4) BSIG-E). The BSI may also require evidence from important entities, provided that assumptions justify the fact that they do not implement or do not correctly implement the legal requirements on IT security. For operators of critical facilities, an already existing obligation to provide evidence is transferred to Section 39 BSIG-E.

On the basis of previous enforcement practice, the Federal Ministry of the Interior and Community (BMI) estimates that the BSI: will require evidence from around 24 (particularly) important institutions per year. According to Online Database of Compliance Costs (OnDEA) (ID 2015030909595501 and 2020093009264402), the existing obligation to provide evidence for operators of critical facilities causes an average time expenditure of 282 hours and material costs of EUR 19,300. With an average wage of EUR 56.94 per hour (see Guidance paper, section 7, economy A-S excluding O; medium qualification level at 6 per cent, high qualification level at 94 per cent; as well as OnDEA ID 2015030909595501 and 2020093009264402), the annual compliance costs for the estimated 24 entities required to provide evidence are approximately EUR 849,000.

bb. Further legislative changes

The draft regulation includes numerous legislative changes with no or no significant impact on the compliance costs (see table, ‘formal amendment’ or ‘minor’). On the one hand, existing requirements will continue in the future versions of the BSIG, the EnWG and the TKG, so that there are no discharges due to the removal of requirements. On the other hand, these requirements may lead to minor increases in expenditure under the future legal situation, as the scope of the BSIG will be extended. Such minor increases result, for example, from Sections 7, 12, 17 and 41 BSIG-E (see BR-Drs for justification on de minimis). 16/21, p. 34), Section 64(5) BSIG-E (when measuring the compliance costs of the IT Security Act and the Act transposing the NIS Directive, the BSI stated that it had carried out only a few checks) or Section 33(3) BSIG-E (according to the BSI, the indication of a functional mailbox is sufficient, cf. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Kontaktstelle-benennen/kontaktstelle-benennen_node.html). Legislative changes with compliance encumbrances are discussed in the previous section (see table, requirement 4.2.X).

Requirement description	Paragraph		StBA ID	Compliance costs
	formerly	future		
BSIG (Article 1)				
Provision of documents and data carriers	Section 4a	Section 7 Paragraph 1	2021012507333201	minor
Inventory data disclosure	Section 5c	Section 12	2021012507393701	minor
Obligation to provide information (manufacturers of information technology products and systems) vis-à-vis the Federal Office	Section 7a (2)	Section 14 Paragraph 2	2021011810433601	formal amendment
Measures (providers of telecommunications services) in connection with orders issued by the Federal Office for the prevention of specific major threats	Section 7c	Section 16	2021011810483101	formal amendment
Costs associated with orders issued by the Federal Office (BSI) vis-à-vis digital service providers	Section 7d	Section 17	2021012507494901	minor
Compliance with a minimum level of IT security (critical infrastructures)	Section 8a in conjunction with Section 8c	Section 31 Paragraph 1	2015030909595401	See Requirement 4.2.1.
Compliance with a minimum level of IT security (digital service providers)	Section 8c (1)	Section 31 Paragraph 1	2017052913283301	See Requirement 4.2.1.
Mandatory use of intrusion detection systems for operators of critical infrastructure	Section 8a (1a)	Section 31 Paragraph 2	2021011810531701	See Requirement 4.2.1.
Notification of significant IT security incidents to the BSI (critical infrastructures)	Section 8b (4)	Section 32	2015030909595201	See Requirement 4.2.2.
Notification of significant IT security incidents to	Section 8c	Section 32	2017052913283701	See Requirement

the BSI (digital service provider)	(3)			4.2.2.
Obligation for undertakings in the particular public interest to report to the BSI without delay certain disruptions to their information technology systems, components and processes	Section 8f(7) and (8)	Section 32	2021012507215301	See Requirement 4.2.2.
Registration of the critical infrastructure and designation of a contact point	Section 8b (3)	Section 33 Paragraph 1	2015030909595901	See Requirement 4.2.3.
Operation of a contact point	Section 8b (3)	Section 33 Paragraph 3	2015030909595701	minor
Demonstration of compliance with minimum requirements through security audits (critical infrastructures)	Section 8a (3)	Section 39 Paragraph 1	2015030909595501	formal amendment
Evidence of measures to safeguard the security of network and information systems (digital service providers)	Section 8c (4)	Section 39 Paragraph 1	2020093009355901	formal amendment
Obligation of companies in the particular public interest to submit a self-declaration on IT security to the BSI	Section 8f(1)	Section 39 Paragraph 1	2021012506571401	formal amendment
Provision of information in the context of the official audit	Section 8f(9)	Section 39 Paragraphs 1 and 64(5)	2021012507544601	formal amendment
Obligation to submit information to the BSI of KRITIS and UBI to deal with significant IT disruptions	Section 8b (4a)	Section 40 Paragraph 5	2021012506532301	See Requirement 4.2.2.
Notification to the BMI of the use of critical components for which a statutory certification obligation exists	Section 9b (1)	Section 41 Paragraph 1	2021012507595001	minor
Manufacturer's guarantee to the critical infrastructure manager	Section 9b (3)	Section 41 Paragraph 2	2021012508035801	minor
Information on security vulnerabilities, malware, attacks or attempted attacks on information technology security and the practices observed	Section 4b (2)	Section 5 Paragraph 4	2021012507365101	formal amendment
Application for a security certificate	Section 9 Paragraph 2	Section 54 Paragraph 2	200609271412501x	formal amendment
Application by conformity assessment bodies for authorisation to act as such	Section 9a (2)	Section 55 Paragraph 2	2021012507302801	formal amendment
On-site monitoring of BSI audits	Section 8a (4)	Sections 64 and 65	2017052913282901	minor
EnWG (Article 16)				
Compliance with a minimum level of IT security (energy)	Section 11 Paragraphs 1a and b	Section 5c(1) and (2)	2020093009264301	See Requirement 4.2.1.
Documentation of compliance with IT security (energy) security requirements	Section 11 Paragraph 1b	Section 5c(1) and (2)	2020093009264402	formal amendment
Reporting significant IT security incidents to BSI (Energy)	Section 11 Paragraph 1c	Section 5c(6) and (7)	2020093009264501	See Requirement 4.2.2.
TKG (Article 23)				
Compliance with a minimum level of IT security (telecommunications)	Section 165 Paragraph 2	Section 165 Paragraphs 2 and 2a	2020093009264401	See Requirement 4.2.1.
Notification of significant IT security incidents to BSI (telecommunications)	Section 168 Paragraphs 1–3	Section 168 Paragraphs 1 to 3	2011101812110109	See Requirement 4.2.2.

SME test

An SME test has been carried out for the draft Act. The proposed scheme concerns small and medium-sized enterprises, as they may fall under Section 28(2) BSIG E. It is expected that around 20,900 companies are expected to be identified as important entities. Burdens on medium-sized enterprises could arise from an initial lack of routine in the implementation of the above-mentioned provisions. It is also to be expected that technical expertise may still be under development for smaller companies.

The draft regulation transposes Directive (EU) 2022/2555 of the European Parliament and of the Council, which is why derogations from the national design are limited. However, it should be borne in mind that differentiations have been reflected in law in the context of the appropriateness of the measures (see above). The proposed regulation offsets the burdens imposed by the frequency with which an obligation must be complied with, varying according to the type of entity.

c. Compliance cost to the administration

The federal administration incurs implementing costs as the addressee of the requirements of the draft regulation on safeguarding security in information technology (cf. requirements 4.3.1 to 4.3.4), whereby requirement 4.3.1, with the exception of the BMVg by the departments and the Federal Chancellery, and requirements 4.3.2 to 4.3.4 are also to be met by the business authorities, federal courts and other federal authorities.

In addition, some authorities also incur further implementing costs, as they are assigned new administrative tasks through several requirements (cf. requirements 4.3.5 to 4.3.12).

In order to estimate the Federal Government's compliance costs, the BMI, together with the StBA, carried out a written survey of the federal administration. In some cases, the StBA received aggregated estimates from departments for the entire business area and partly obtained individual estimates for individual authorities.

Due to the predictive nature of the data, many bodies involved emphasise that the information is sometimes subject to high uncertainty.

Below is a description of the compliance cost estimate for government agencies for each specification. The presentation is highly aggregated, as individual data on the need to upgrade the IT security of federal administration entities are to be classified as sensitive. The qualitative description is a much shortened but mutatis mutandis synthesis of the relevant explanations provided by the bodies involved.

In the transitional phase immediately after the entry into force of the Act, several requirements involve one-off activities, including for the implementation of new processes. The resulting expenditure is recorded as one-off compliance costs. Subsequent permanent activities and resulting expenditure are presented as annual implementing costs.

aa. Substantial legislative amendment

aaa. Requirements for federal administration entities for maintaining IT security

The authorities estimate their permanent staffing needs from requirements (4.3.1 to 4.3.4) for maintaining IT security at around 381 posts, resulting in staff costs of around 31.7 million euro. They estimate the total annual material costs at around EUR 30 million. The total one-off compliance costs are 27 million euro.

Requirement 4.3.1: Measures to safeguard the security of the information; Section 43 Paragraphs 1, 3 and 4, sentence 2, Sections 44 to 46 and 50 in conjunction with Sections 29 and 37(1) and Section 46(4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases*	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
11.0 (mD)	1,600	33.80	0	595	0
108.8 (gD)	1,600	46.50	0	8095	0

47.4 (hD)	1,600	70.50	0	5347	0
1	0	0	14,364,065	0	14,364
Change in compliance costs (in EUR thousand)				28,400	

* mD ~ intermediate service, gD ~ senior service, hD ~ higher service

One-off compliance costs for the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
5.8 (mD)	1,600	33.80	0	314	0
49.9 (gD)	1,600	46.50	0	3,713	0
21.7 (hD)	1,600	70.50	0	2,448	0
1	0	0	9,832,553		
Compliance costs (in thousands EUR)				16,307	

Federal administrative entities within the meaning of Section 29 BSIG-E must in future create the conditions for ensuring information security with regard to IT operations in accordance with Section 43(1) BSIG-E. To this end, the BSI is to lay down the requirements to be met by means of IT baseline protection and minimum standards for security in federal information technology (cf. Section 44 BSIG-E). A fundamental obligation to implement minimum standards for the security of information technology already exists under current law (cf. Section 8 BSIG) and was last extended to IT service providers in so far as they provide IT services for the federal communications technology (cf. BT-Drs. 19/26106, p. 78 and OnDEA, among others ID 2,021,012,607,002,101).

The federal administration entities permanently estimate the total staffing needs at 167 posts and one-off 77 posts, resulting in annual staff costs of around 14 million euro and six million euros once.

Staff costs arise from, inter alia, the following activities: Establishing and implementing risk management in the field of information security, drawing up and updating security policies, security incident management, ensuring compliance with information security requirements by service providers and in the procurement, development and maintenance of IT systems, extended reporting, development and supervision.

Annual and one-off material costs are estimated by the federal administration institutions at around EUR 14 million and ten million euros respectively. In addition to individual items such as the cost of acquiring and maintaining the expertise of the Information Security Officer and representing it, there are material costs, in particular for the development and operation of the additional IT infrastructure required and for the use of third-party services.

Significant infrastructure cost items include: Additional hardware, support and maintenance of hardware, software and licences, upgrade and continuous operation of parallel infrastructure and redundant operating environments, and communication structures.

Some significant expenditure on consultancy services is appreciated by public authorities with reference to the general shortage of skilled workers and the comparatively attractive salaries of the private sector. In general terms, contracts and services are to be provided in various areas of information technology in accordance with the requirements of the Implementing Act. More specifically, for example, BSI will be contracted to external consultants that will be used, inter alia, for IS penetration kits (and assessment of shortcomings) and for the specific expertise in security advice on critical business processes and IT procedures. Likewise, coaching, support services for, inter alia, the preparation of the security

policy and the verification of IT service providers and support from third parties for emergency management will be purchased.

The compliance costs are EUR 28 million per year and EUR 16 million once.

Requirement 4.3.2: Security incidents (reporting; remedial measures; information obligations); Sections 10, 32, 35 and 36 in conjunction with Sections 29, 37, 43(5) and (6) and 46(4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
12.9 (mD)	1,600	33.80	0	697	0
87.7 (gD)	1,600	46.50	0	6506	0
26.6 (hD)	1,600	70.50	0	3001	0
1	0	0	8,928,570	0	8,929
Change in compliance costs (in EUR thousand)				19,603	

One-off compliance costs for the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
0.2 (mD)	1,600	33.80	0	11	0
2.1 (gD)	1,600	46.50	0	156	0
8.2 (hD)	1,600	70.50	0	925	0
1	0	0	4,138,693	0	4,139
Compliance costs (in thousands EUR)				5,231	

Federal administration entities must report significant security incidents to the BSI (cf. Section 32 in conjunction with Section 29(2) BSIG-E). With the exception of the scope of the Federal Defence Department, in the event of a BSI order, they must take measures to prevent or remedy security incidents (cf. Section 10 in conjunction with Section 29(2) and (3) BSIG-E) and, if the BSI instructs recipients of their services, inform recipients of their services of significant security incidents (cf. Section 35 in conjunction with Section 29(2) and (3) BSIG-E).

A total of 10.5 posts and 127.2 permanent posts will probably be used to meet the requirements for security incidents, resulting in staff costs of 1.1 million euro once and 10.2 million euro per year. Processing costs are likely to arise in particular for the implementation of the orders for measures to prevent and remedy security incidents. The reports themselves and the reporting of the implementation of the orders to the BSI also involve time.

Material costs are estimated at around EUR 4.1 million once and around EUR 8.9 million per year. These are related to incident and IT security incident management, emergency management and material implementation of security measures to prevent and resolve security incidents. Some authorities also expect external expert teams to be deployed.

The compliance costs amount to EUR 5.2 million once and 19.1 million euro per year.

Requirement 4.3.3: Regular training; Section 43 (2) and Section 44(1) in conjunction with Sections 29, 37 and 46(4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
4.4 (mD)	1,600	33.80	0	238	0
17.6 (gD)	1,600	46.50	0	1,309	0
9.7 (hD)	1,600	70.50	0	1,094	0
1	0	0	2,500,752	0	2,501
Change in compliance costs (in EUR thousand)				5,142	

One-off compliance costs for the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
0.0 (mD)	1,600	33.80	0	0	0
2.8 (gD)	1,600	46.50	0	208	0
0.6 (hD)	1,600	70.50	0	68	0
1	0	0	663,000	0	663
Compliance costs (in thousands EUR)				939	

The heads of establishment of the federal authorities are to undergo cybersecurity training on a regular basis (cf. Section 43(2) BISG-E). In accordance with Article 20(2) of the NIS 2 Directive, the training obligation also extends to all staff – this is ensured in national law by Section 44(1) BSIG-E (see explanatory memorandum).

The federal authorities estimate the total human resources required for attending further training and the partial development of teaching materials at around 3.4 posts initially and on a permanent basis at around 31.7 posts. Material costs for teaching materials, training and the partial planned involvement of external teachers and experts are estimated once at EUR 663,000 and EUR 2.5 million on an ongoing basis. The compliance costs are EUR 939,000 once and 5.1 million euro per year.

Requirement 4.3.4: Major digitalisation projects and communication infrastructures; Section 47 BSIG-E in conjunction with Sections 29, 37 and 46(4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
4.3 (mD)	1,600	33.80	0	233	0
28.1 (gD)	1,600	46.50	0	2,091	0
22.4 (hD)	1,600	70.50	0	2,527	0
1	0	0	4,579,962	0	4,580
Change in compliance costs (in EUR thousand)				9,430	

One-off compliance costs for the Federal Government: 4.7 EUR million

For the planning and implementation of major digitisation projects and communication infrastructures of the Federal Government, its own information security officers shall be appointed. In order to ensure information security in such projects, means of information security must be used to meet the needs (cf. Section 47 BSIG-E).

The number of significant digitalisation projects and communication infrastructures varies greatly between public authorities. A large number of authorities see no effort in this regard because of the lack of projects. Some authorities, such as the Federal Environment Agency, the General Customs Directorate, the Federal Foreign Office or the Federal Statistical Office, expect several projects on a permanent basis. In order to ensure the information security of projects, such authorities often expect one entity per project, including across careers.

In total, the federal authorities estimate the need for posts on a permanent basis at 55, resulting in annual staff costs of EUR 4.9 million. They estimate the material costs at EUR 4.6 million per year and once at around 4.7 million euro. These are mainly due to the use of third party services (e.g. for the preparation and initialisation of security guidelines on key digitisation projects, as well as for external operational support in the absence of available qualified staff) and the development and operation of additional IT infrastructure.

The compliance costs amount to EUR 4.7 million once and 9.4 million euro per year.

bbb. Enforcement requirements

The implementing law restructures the remit of the relevant enforcement authorities in the BSIG. Significant new costs are created by BSI, BBK, BNetzA, BfDI and BMI. This is mainly due to the rapidly increasing number of entities to be supervised. At present, it is difficult to estimate the actual additional staffing needs of the enforcement authorities concerned. The authorities estimate their total permanent staffing needs at around 539 posts, resulting in annual staff costs of around 50 million euro. The total annual or one-off material costs are estimated at around ten million euro and eleven million euro respectively.

The BSI alone accounts for around 476 posts (in addition to 16 other posts which are taken into account in requirements 4.3.1 to 4.3.4). By comparison, the BSI alone currently employs around 645 people to fulfil the existing task of information technology security in accordance with Sections 3 et seq. of the Federal Office for Information Security Act (BSIG) due to the previous regulatory projects IT Security Act, Act on the Implementation of Directive (EU) 2016/1148 and the Second Act on strengthening the security of information technology systems.

Many of the authorities, which are already involved in the implementation of the BSIG to a relatively small extent, have not indicated any significant changes in their enforcement burden. These legislative amendments may be regarded as formal legislative changes for the purpose of implementing costs (see sub-section (b)).

Requirement 4.3.5: Fundamental tasks and powers (BSI, BfDI); Sections 3 to 19 in conjunction with Sections 20 to 27 BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
26.0 (mD)	1,600	33.80	0	1,406	0
96.0 (gD)	1,600	46.50	0	7,142	0

187.0 (hD)	1,600	70.50	0	21,094	0
1		0	3,943,000	0	3,943
Change in compliance costs (in EUR thousand)				33,585	

One-off compliance costs for the Federal Government: 2.5 EUR million

The ‘fundamental tasks’ and powers in the area of information technology security regulated by federal law will in future arise from Sections 3 to 19 in conjunction with Sections 20 to 27 BSIG-E. The BSI already carries out comprehensive tasks in this area (cf. Section 3 BISG; OnDEA, including ID 2015030910484001, 2021012608550401). The implementation of the NIS 2 Directive will extend these tasks of the BSI. For example, in the future, all federal administrative entities will fall within the scope of the BSIG, which in particular increases the cost of activities aimed at safeguarding the protection of the entire federal communications technology (cf. §Section 7 and 8 BSIG-E). With regard to data protection matters, the BSI is assisted by the BfDI in carrying out its tasks under the BSIG. The BfDI sees the considerable expansion of the scope of the BSI’s activities and the extension of its tasks to a much greater number of authorities in terms of advice and supervision by the BfDI vis-à-vis the BSI.

In total, the BfDI puts its permanent additional effort at four posts (two posts each in the intermediate and senior civil service) and the BSI at 305 posts (around 26, 94 and 185 posts in the intermediate, senior and higher civil service respectively). This results in annual personnel costs of around EUR 33.6 million across authorities. More specifically, the needs arise from activities such as: Advice and control to ensure the data protection-compliant implementation of the NIS 2 Implementation and Cybersecurity Enhancement Act, drafting, aligning and regularly adapting guidelines on the definition of significant incidents due to the dynamics of developments in cyber-attacks. The deployment of BSI Computer Emergency Response Teams in support of other teams on the territory of the Union shall be provided and deployed accordingly; this allows the mutual assistance services provided for in the law to be provided within the Union in addition to existing operations within the national framework. There is also a need for peer reviews, operational coordination, CSIRTs single point of contact, notification of entities, extensive incident support, messaging warnings, permanent services, information by LZ/WG, online portal with WG23, scanning of vulnerabilities).

For the implementation and operation of the new procedures and additional IT equipment associated with the additional tasks (e.g. upgrading the detection infrastructure, updating/extension of the training concept for KRITIS auditors, audits, public relations), the authorities together estimate annual or one-off material costs of around EUR 4 million and 2.5 million respectively.

The compliance costs amount to EUR 2.5 million once and 33.6 million euro per year.

Requirement 4.3.6: Handling reports of significant security incidents (BSI and BBK); Sections 32, 35, 36 and 40(3) and (4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
12.0 (mD)	1,600	33.80	0	649	0
49.0 (gD)	1,600	46.50	0	3,646	0
49.0 (hD)	1,600	70.50	0	5,527	0
1	0	0	1,119,450	0	1,119

Change in compliance costs (in EUR thousand)	10,941

One-off compliance costs for the Federal Government: 508,000 EUR

Already today, the BSI is a single point of contact for reporting from critical infrastructure operators of significant security incidents (cf. Section 8b(3) BSIG). In future Sections 32, 35, 36, 40(4) and (5) BSIG-E govern the implementation tasks of the BSI and the BBK in this regard. On the part of the authorities, considerable additional work is to be expected simply due to the significant expansion of the entities subject to reporting requirements. In addition, the average cost per report will be higher, as a multi-stage reporting procedure will now be introduced (cf. Section 32 BSIG-E, Preliminary 4.2.2). In certain cases, the BSI can issue instructions on how to inform service recipients (cf. Section 35 BSIG-E) and provides guidance on reporting to law enforcement authorities in criminal law cases (cf. Section 36 BSIG-E). In addition, the BSI may request certain information from operators and in certain cases it is itself subject to a notification obligation vis-à-vis Member States of the European Union (cf. Section 40(3) and (4) BSIG-E). The BBK sees an additional burden as a result of the establishment and operation of the reporting procedure. In addition, there is an additional burden, as checks on IT-SIG 2.0 must be carried out for possible conflicts with Section 12(1) KRITIS-DachG-E Reporting.

In total, the BBK estimates its permanent additional expenditure at six posts (two posts each in the middle, senior and higher civil service); the BSI expects that an additional 104 posts will be needed across all careers (10, 47 or 47 posts in the middle, senior and higher civil service); This results in annual personnel costs of around EUR 9.8 million across authorities. In addition, according to BBK and BSI, there are one-off and annual material costs of EUR 508,000 and EUR 1.1 million respectively for the establishment and operation of the notification tool, the development of the reporting system, new notebooks and the scaling up of communication and support measures.

Requirement 4.3.7: Establishment and operation of a register for (particularly) important entities, certain types of entities and for federal administration entities (BSI and BBK); Sections 33, 34 and 43(4) BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
7.0 (mD)	1,600	33.80	0	379	0
12.0 (gD)	1,600	46.50	0	893	0
7.0 (hD)	1,600	70.50	0	790	0
1	0	0	1,950	0	2
Change in compliance costs (in EUR thousand)				2,063	

One-off compliance costs for the Federal Government: 8,000 EUR

The BSI and BBK incur compliance costs as a result of the registration obligation for (particularly) important entities, certain types of entities and federal administration entities (cf. Sections 33, 34 and 43(4) in BSIG-E). The BSI already processes and maintains corresponding information from critical infrastructure operators and undertakings in the particular public interest (cf. Sections 8b(3) and 8f(5) BSIG).

According to the BBK, the new rules require the establishment and permanent implementation of an adapted registration procedure. In addition, there is an additional burden as checks on IT-SIG 2.0 for possible conflicts with Section 6(1) KRITIS-DachG-E registration must be carried out. As a result of the extension of the scope of the legislation, the BSI ex-

pects additional efforts, in particular through the processing of incoming registrations, processing requests and master data maintenance of particularly important and important entities. It is also responsible for the specialist administration of IT systems. BSI and BBK estimate the total additional staffing needs at 26 posts (six in the BBK and 20 in the BSI), resulting in permanent staff costs of around two million euros. In addition, low material costs are incurred for the initial purchase and permanent replacement of notebooks.

Requirement 4.3.8: Single reporting and contact point (BSI, BBK, BNetzA); Section 40 BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
3.0 (mD)	1,600	33.80	0	162	0
14.0 (gD)	1,600	46.50	0	1,042	0
26.5 (hD)	1,600	70.50	0	2,989	0
1	0	0	2,925	0	3
Change in compliance costs (in EUR thousand)				4,196	

One-off compliance costs for the Federal Government: 11,700 EUR

Section 40 BSIG-E continues the task of the BSI as a single reporting and contact point, as previously laid down in Section 8b BSIG, with the support of the BBK. The significant extension of the scope of the BSIG creates additional costs for the authorities: In particular, for the collection of information on IT-related security and its technical evaluation in view of the impact on critical services, audits in relation to IT-SIG 2.0 on possible conflicts with incident reports and processing pursuant to Section 12(5) to (8) of the KRITIS-DachG-E, adaptation of the reporting unit's processes also taking into account KRITS-DachG-E. In the telecommunications sector, the Federal Network Agency also counts as a reporting and contact point. To cooperate, the latter must set up a body which is available to the BSI as a contact point and, if necessary, analyses the necessary information and provides it without delay.

BSI, BBK and BNetzA estimate the additional staffing needs at a total of 44 posts (seven in BBK, around 33 in BSI and four in BNetzA), resulting in permanent staff costs of around EUR 4.2 million. In addition, low material costs are incurred for the initial purchase and permanent replacement of notebooks.

Requirement 4.3.9: Various enforcement tasks in the area of IT security – Federal Government (BMI, BSI and BBK); Section 30 (9), Sections 39, 48, 58, 61 to 64 and 65 BSIG-E

Change in annual compliance costs of the Federal Government:

Number of cases	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
4.0 (mD)	1,600	33.80	0	216	0
10.8 (gD)	1,600	46.50	0	804	0
13.0 (hD)	1,600	70.50	0	1,466	0
1	0	0	2,535,425	0	2,535
Change in compliance costs (in EUR thousand)				5,022	

One-off compliance costs for the Federal Government: 11,700 EUR

In addition to the tasks previously referred to, the BMI, the BSI and the BBK will be entrusted with another task by the draft regulation. These include the processing of applications for the qualification of sector-specific standards (cf. Section 30(9) BSIG-E), the processing and verification of evidence of compliance with the legal requirements on IT security (cf. Section 39 BSIG-E), the taking of supervisory and enforcement measures (cf. Sections 61-64 BSIG-E) and the conduct of administrative offence proceedings (cf. 65 BSIG-E).

Across authorities, the authorities concerned estimate the staffing needs for the various tasks at around 28 posts (around eight, six and 14 posts at BMI, BBK and BSI respectively), resulting in permanent staff costs of 2.5 million euro. In addition, there are annual material costs of EUR 2.5 million, mainly for studies, according to the BSI, and low one-off material costs.

Requirement 4.3.10: Various enforcement tasks in the area of IT security – Länder; Section 40 (3)(2) and Section 61(9)(2) BSIG-E

Change in annual compliance costs of the Länder: 85 000 EUR

In principle, two legislative changes affect the implementation burden of the Länder:

Essential information for the prevention of risks to security in information technology must be transmitted by the BSI to competent Land authorities, which will then analyse the relevance together with other authorities (cf. Section 40(3)(2) BSIG-E). In the past, there have been 15 of these notifications on operators of critical infrastructure and digital service providers per year. Due to the extension of the scope to particularly important and important entities, it can be cautiously estimated (cf. requirement 4.2.1) that the number of relevant notifications increases five times, i.e. an additional 75 cases. According to the guidance document, two working days are estimated as the case-related time required to receive and analyse a report (see Guidance document, Annex 9, standard activities 1 and 2 in simple complexity, 4, 8, 9 and 14 in medium complexity and 5 in high complexity). Processing is assumed by the higher service, resulting in a total annual additional cost of EUR 85,000 at a rate of EUR 70.50 per hour.

Finally, the competent Land authority may, in certain cases, temporarily prohibit the exercise of its activity by the senior management (cf. Section 61(9)(2) BSIG-E). It can be assumed that this measure will occur extremely rarely as a last resort and that the other supervisory measures are generally sufficient. In this respect, the compliance costs are considered negligible due to the extension of the scope.

Requirement 4.3.11: Basic IT security tasks in the energy sector (BNetzA); Sections 5c and 95 EnWG-E

Change in annual compliance costs of the Federal Government:

Number of cases*	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
0.8 (mD)	1,600	33.80	0	43	0
4.8 (gD)	1,600	46.50	0	357	0
5.2 (hD)	1,600	70.50	0	587	0
Change in compliance costs (in EUR thousand)				987	

In the energy sector, the provisions on IT security for operators of energy supply networks and energy installations from Section 11(1a) to (1g) of the EnWG are recast in Section 5c

EnWG-E. BNetzA will incur a new burden in this respect as the existing IT security catalogues and requirements on risk treatment plans and on addressing safety deficiencies will be extended. It must develop and maintain new training concepts, conduct energy system assessments of BSI messages and transmit these results to the BSI, prepare annual reports on security incidents and carry out additional misdemeanour procedures. Overall, BNetzA expects an additional staffing requirement of 10.8 posts across careers, resulting in an annual implementation cost of almost one million euros.

Requirement 4.3.12: Basic IT security tasks in the telecommunications sector (BNetzA); Sections 165 and 168 TKG-E

Change in annual compliance costs of the Federal Government:

Number of cases*	Time spent per case (in hours)	Hourly wage (in EUR)	Material costs per case (in EUR)	Staff costs (in thousands of EUR)	Material costs (in thousands of EUR)
1.0 (mD)	1,600	33.80	0	54	0
10.0 (gD)	1,600	46.50	0	744	0
1.0 (hD)	1,600	70.50	0	113	0
1	0	0	2,000,000	0	-2,000
Change in compliance costs (in EUR thousands)				2,911	

One-off compliance costs for the Federal Government: 8 EUR million

In the telecommunications sector, measures for operators of public telecommunications networks and providers of publicly available telecommunications services are extended in accordance with Section 165 of the Telecommunications Act-E in the form of concepts, supply chain indications, encryption procedures and assessments of measures to be fulfilled by particularly important and important entities. These are reviewed by BNetzA on a rolling basis every two years. In addition, regular further training and courses must be provided in order to keep up-to-date in the field. Section 168 of the TKG-E is extended, as an initial notification and a final report are now provided for. The reports must be evaluated and assessed, if obliged entities fail to perform their duties during the period, an administrative offence procedure must be carried out. BNetzA estimates the additional human resources at 12 posts on a permanent basis, resulting in an annual cost of EUR 911,000.

In addition, according to BNetzA, material costs of eight million euros are incurred on a one-off basis and two million euros annually, because of the sometimes highly sensitive data reported by telecommunications service providers, a non-existent CI registry has to be established and operated.

bb. Further legislative changes

As in the case of industry, it is assumed that the registration burden (cf. Section 33 in conjunction with Section 29 BSIG-E) will be negligible. In addition, many requirements are transferred from the current version to the future version of the BSIG or EnWG, without the authorities concerned seeing any changes in compliance costs (see table, 'formal amendment'). Legislative changes with compliance encumbrances are discussed in the previous section (see table, requirement 4.3.X).

Requirement description	Paragraph		StBA ID	Compliance costs
	formerly	future		
BSIG (Article 1)				
Technical supervision of the BSI	Section 1	Section 1	2017052913284101	formal amendment
Information to the Committee on the Internal Affairs on the application of the BSIG (BMI)	Section 13 Paragraph 3	Section 58 Paragraph 3	2023121812242201	formal amendment

Requirement description	Paragraph		StBA ID	Compliance costs
Administrative offence proceedings (BSI)	Section 14	Section 65	2021012613125701	Requirement 4.3.10.
Involvement in administrative infringement proceedings of the BSI (BMG)	Section 14	Section 65	2021012707301701	formal amendment
Agreement procedure between the social security supervisory authorities (BMAS and BAS) with BSI on measures to be taken	Section 14a	Section 64	2021102813021101	formal amendment
Designation of KRITIS operators	Section 2 (10) in conjunction with Section 10(1)	Section 28 (6) and (7)	2023121812504101	formal amendment
Ensuring IT security in communication between public authorities and public networks (ITZBund)	Section 2 Paragraph 3	Section 7 in conjunction with Section 2(1)(20)	2021110314194701	Requirement 4.3.6
Contribute to the promotion of information technology security by BSI (BMFSFJ)	Section 3 Paragraph 1	Section 3 Paragraph 1	2021012707534101	formal amendment
Contribute to the promotion of information technology security by BSI (BzKJ)	Section 3 Paragraph 1	Section 3 Paragraph 1	2021012708221801	formal amendment
Contribute to the promotion of information technology security by BSI (BAFzA)	Section 3 Paragraph 1	Section 3 Paragraph 1	2021012709053401	formal amendment
Advice, information, recommendation and warning on information technology security issues (BSI)	Section 3 (1), subparagraphs 14, 14a and 19	Section 3 Paragraph 1	2015030910484001	Requirement 4.3.6
Advice, control and audit of data protection requirements in the implementation of the BSI's (BfDI) audit, consultation and control powers	Section 3 (1), sentence 2, subparagraph 12	Section 3 Paragraph 1	2021012706485901	Requirement 4.3.6
Control of federal communication technology by the Federal Office (BSI)	Section 4a	Section 7	2021012608550401	Requirement 4.3.6
Participation in the control of federal communication technology by the BSI (Federal authorities)	Section 4a	Section 7	2021012707130301	Requirement 4.3.6
General Information Security Referral Unit (BSI)	Section 4b	Section 5 Paragraph 1	2021012609014501	Requirement 4.3.6
Participation in the General Reporting Unit for Information Security at the BSI (Federal Authorities)	Section 4b	Section 5 Paragraph 1	2021012707162401	formal amendment
Protection against malware and threats to federal communications technology (BSI)	Section 5	Section 8	2021012609055001	Requirement 4.3.6
Contribute to the processing of own internal logging data by the BSI (Federal Authorities)	Section 5a	Section 9	2021012606533701	formal amendment
Processing of internal logging data (BSI)	Section 5a	Section 9	2021012609332401	Requirement 4.3.6
Restoring the security or functioning of information technology systems in exceptional cases (BSI)	Section 5b	Section 11	2021012609372701	Requirement 4.3.6
Inventory data query (BSI)	Section 5c	Section 12	2021012609432501	Requirement 4.3.6
Tasks related to the restriction of information obligations (BSI)	Section 6a	Section 21	2019011110030201	Requirement 4.3.6
Technical investigations by the Federal Office (BSI)	Section 7a	Section 14 Paragraph 1	2021012610373001	Requirement 4.3.6
Implementation of information technology security measures (BMAS)	Section 7a	Section 14	2021102713464901	formal amendment
Contribute to the investigation of information technology security by BSI (BfDI)	Section 7a(3)	Section 14 Paragraph 3	2021012706565501	Requirement 4.3.6
Contribute to the investigation of information technology security by BSI (BMG)	Section 7a(3)	Section 14 Paragraph 3	2021012707245801	formal amendment
Detection of security risks for network and IT security and attack methods (BSI)	Section 7b	Section 15	2021012610415601	Requirement 4.3.6
Agreement with the BfDI prior to an order is issued by the Federal Office (BSI)	Section 7c(1)	Section 16 Paragraph 1	2021012707021901	Requirement 4.3.6
Establishment of minimum standards for the security of federal information technology at the BSI	Section 8	Section 44	2021012611515101	Requirement 4.3.6
Establishment and compliance with agreed minimum IT standards and involvement of the BSI in major digitalisation projects (Federal	Section 8 paragraphs 1, 1a and 4	Section 44 in conjunction with Sec-	2021012607002101	formal amendment

Requirement description	Paragraph	tion 47	StBA ID	Compliance costs
Examination of industry-specific safety standards (BSI)	Section 8a	Section 30 Paragraph 9	2023121812331001	Requirement 4.3.6
Implementation of organisational and technical arrangements (AA)	Section 8a(1a)	Section 31 Paragraph 2	2021102814224601	formal amendment
Contribute to the audit of industry-specific safety standards (BBK)	Section 8a(2)	Section 30 Paragraph 9	2015030910484201	formal amendment
Contribute to the fulfilment of the tasks of the reporting unit (BfV)	Section 8b(2), subparagraph 4b	Section 40 (3), subparagraph 5	2015030910484401	formal amendment
Contribute to the fulfilment of the tasks of the reporting unit (BND)	Section 8b(2), subparagraph 4b	Section 40 (3), subparagraph 5	2015030910484501	formal amendment
Assessment and management of significant security incidents (BSI)	Section 8b(4a)	Section 40 Paragraph 5	2021012611561201	Requirement 4.3.7
Contribute to the management of significant security incidents (Federal Authorities)	Section 8b(4a)	Sections 36 and 40(5)	2021012710391601	Requirement 4.3.7
Contribute to the management of significant security incidents (ITZBund)	Section 8b(4a)	Sections 36 and 40(5)	2021110314022901	Requirement 4.3.7
Processing of self-declarations (BSI)	Section 8f	Sections 33 and 34	2021012611593401	Requirement 4.3.3
National Cybersecurity Certification Authority (BSI)	Section 9a	Section 54	2021012612594401	formal amendment
Contribute to the critical component ban test (BMI)	Section 9b	Section 41 Paragraph 3	2021012613034601	formal amendment
Contribute to the verification of the guarantee statement and prohibition of critical components (BNDs)	Section 9b(3) and (4)	Section 41 (3) and (4)	2021110409335901	formal amendment
Prohibiting the use of critical components or issuing other orders (BMI)	Section 9b(4)	Section 41 Paragraph 4	2021012508360401	formal amendment
Contribute to the prohibition of critical components (BMG)	Section 9b(4)	Section 41 Paragraph 4	2021012707270601	formal amendment
Contribute to the prohibition of critical components (BMAS)	Section 9b(4)	Section 41 Paragraph 4	2021102714324301	formal amendment
Contribute to the prohibition of critical components (AA)	Section 9b(4)	Section 41 Paragraph 4	2021110111334101	formal amendment
Issuing the IT security label by the Federal Office (BSI)	Section 9c	Section 55	2021012613071901	formal amendment
Adjustments to IT security (DGZ)	Sections 4a, 4b, 8, 8b(4a)	Section 5 Paragraph 3	2021110111534201	Requirement 4.3.1
Tasks related to the restriction of data subjects' rights (BSI)	Sections 6b to 6f	Sections 23 to 27	2019011110030202	Requirement 4.3.6
EnWG (Article 15)				
Processing of evidence from critical companies on compliance with BSI requirements (BNetzA)	Section 11 Paragraph 1e	Section 5c(4)	2021110811522901	formal amendment
Definition of security requirements (BNetzA)	Section 11 Paragraph 1g	Section 5c	2022063010393601	formal amendment

5. Additional costs

None.

6. Other consequences of the legislation

The draft law increases security of supply for consumers. The existing provisions of the BSI Act on Consumer Protection are not affected.

The rules of the draft Act are gender-neutral on the basis of the primary direct concern to the target group of the scheme and therefore without any relevance to equality. However, further strengthening and promoting cyber and information security affects both women and men, both indirectly and directly. Section 4 Paragraph 3, sentence (1) of the Federal Equality Act provides that federal laws, regulations and administrative provisions must

also express equality between women and men in linguistic terms. This has been taken into account in the development of the legislative formulation, taking into account the dication already given.

The rules also meet the requirements of the ‘equivalence check’. The draft law promotes the provision of digital infrastructure and accessibility of services and administrative services. It also takes into account the protection of services of general interest with their different areas, which are an essential prerequisite for equal living conditions for people and social cohesion. There is no expected impact on the existing settlement and spatial structure or demographic concerns.

VII. Executive Footprint

The content of the draft law has not substantially changed as a result of presentations by interest representatives and third parties mandated by the Federal Government.

VIII. Time limit; Evaluation

The law is not subject to a time limit.

In accordance with Article 40 of the NIS 2 Directive, the European Commission shall carry out its own evaluation of the Directive. Accordingly, by 17 October 2027, and every 36 months thereafter, the European Commission shall regularly review the application of the NIS 2 Directive and report to the European Parliament and the Council.

In the light of the results of the European Commission, a comprehensive evaluation of the measures under this Act should be carried out no later than five years. The aim is to assess whether an increase in the common level of cybersecurity has been achieved in Germany. The criterion may be the cybersecurity measures taken by the entities covered by this Act. Information can be obtained from the Federal Office for Information Security (BSI) reporting and from voluntary surveys of the institutions concerned.

After three years at the latest, a comprehensive evaluation of Section 28(6) of the BSI Act is to be carried out. In particular, the aim is to evaluate whether the exemption of KRITIS operators in the financial sector from the reporting obligation under Section 32 has resulted in a lack of essential information for a comprehensive situational picture.

B. Specific part

Re Article 1 (Act on the Federal Office for Information Security and on Information Technology Security of Entities)

The Amendment to the law heading by adding ‘and on Information Technology Security of Entities’ is intended to take account of the fact that this is not purely an Act establishing a federal authority.

The creation of a (official) table of contents is based on the increased scope of the law and the structure of the Act into parts and chapters to facilitate the overview for the user of the law.

Re Part 1 (General provisions)

Re Section 1 (Federal Office for Information Security)

Section 1 continues the previous Section 1.

Re Section 2 (Definitions)

The definitions are designed in numbers rather than individual paragraphs, which are sorted alphabetically, in order to improve clarity. This has become necessary as a result of the introduction of many new definitions due to the requirements of the NIS 2 Directive. Thematic sorting is ruled out because of the large number of terms, and it would no longer be possible to ensure clarity for legal practitioners.

Re subparagraph 1

The definition transposes Article 6(5) of the NIS 2 Directive. The legal definition of a near misses is deliberately broad, as in principle multiple incidents in the context of cybersecurity can be regarded as a near miss. Thus, for example, a professionally designed phishing mail, which was only identified as a result of a particularly high level of awareness among the staff or because of the increased attention of the workforce, may well be regarded as a near misses if it would not have been detected under other normal conditions. However, regular and day-to-day disturbances and nuisances such as spam emails or emails clearly recognisable as phishing mail, even for untrained staff, are not to be regarded as a near miss.

The definition includes the triad of availability, integrity and confidentiality of the previous definition in Section 2(2), sentence 4 of the BSI Act (Information Technology Security). The term ‘authenticity’ is a subset of integrity in German law and therefore, unlike e.g. Article 6(5) of the NIS 2 Directive, there is no explicit mention of the term.

Re subparagraph 2

The definition transposes Article 28(5) NIS 2 Directive and defines ‘legitimate access seekers’ for the purposes of: Section 50.

Re subparagraph 3

The space sector includes, in particular, entities whose functioning is imperative for the provision of various critical services. For this purpose, the terms ‘ground-based infrastructure’ and ‘space-based services’ (Point 45) are defined. Ground-based infrastructure includes entities such as satellite control centres and ground stations, while space-based services, such as Global Navigation Satellite Systems (GNSS) or high-precision time services. The control in the definition of ‘round-based infrastructure’ includes, in particular, communication, observation and control.

Re subparagraph 4

The definition transposes Article 6(30) of the NIS 2 Directive.

Re subparagraph 5

The definition transposes Article 6(32) of the NIS 2 Directive. The provision of digital content and services for Internet users on behalf of content and service providers includes, in particular, so-called ‘caching’. The word ‘service’ refers to actual service rather than formal service.

Re subparagraph 6

The definition transposes Article 6(10) of the NIS 2 Directive.

Re subparagraph 7

The definition continues the previous Section 2(9).

Re subparagraph 8

The definition transposes Article 6(20) of the NIS 2 Directive.

Re subparagraph 9

The definition transposes Article 6(22) of the NIS 2 Directive.

Re subparagraph 10

The definition transposes Article 6(11) of the NIS 2 Directive.

Re subparagraph 11

The definition transposes Article 23(3) and Article 23(11)(2) of the NIS 2 Directive. In the case of the financial losses referred to here, minor damage is regularly excluded.

Re subparagraph 12

The definition transposes Article 6(41) of the NIS 2 Directive. A primary objective within the meaning of the provision is likely to be met if 50 % of the total activity has been exceeded.

Re subparagraph 13

The definition transposes Article 20 of the NIS 2 Directive. Since the duties and powers of the management of federal institutions are regulated differently in: Section 43 in accordance with Section 29, they are explicitly excluded from the definition here.

Re subparagraph 14

The definition transposes Article 6(13) of the NIS 2 Directive. ‘ICT service’ in Regulation (EU) 2019/881 means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.

Re subparagraph 15

The definition transposes Article 6(12) of the NIS 2 Directive. ‘ICT product’ in Regulation (EU) 2019/881 means an element or a group of elements of a network or information system. The term is being introduced to harmonise terminology across Europe in the context of the implementation of the NIS 2 Directive and replaces the old term of IT product in Section 2(9a) of the BSI Act (old version). In terms of content, there are no differences between the two terms. The definition referred to here covers both hardware products and software products.

Re subparagraph 16

The definition transposes Article 6(14) of the NIS 2 Directive. With the term ‘ICT process’, Regulation (EU) 2019/881 refers to any activity performed to design, develop, deliver or maintain an ICT product or ICT service.

Re subparagraph 17

The term information security has already been used in the BSI Act, but has not been defined by law. For the sake of clarity, a corresponding legal definition is now provided, which is based on the already established definitions in the BSI IT basic protection.

Re subparagraph 18

The definition continues the previous Section 2(1).

Re subparagraph 19

The definition continues the legal definition in the previous 14a, sentence 1, the term is now used in Sections 29 and 64. In order to complete the previous legal definition, the German Statutory Accident Insurance (Deutsche Gesetzliche Unfallversicherung e.V.) has been supplemented.

Re subparagraph 20

The definition transposes Article 6(18) of the NIS 2 Directive.

Re subparagraph 21

The definition continues the previous Section 2(3). A consolidation of terms has been carried out, instead of ‘federal authorities’, it is now ‘federal administration entities’. The term is defined by the scope of application of Section 29. The extension of the definition is necessary in the context of the turning point and is necessary in view of the fact that, given the complex digital infrastructure, information technology that is not directly operated or used by federal authorities may also be vulnerable. A compromise of the systems of a federal administration entity is likely to represent a risk for all the entities connected with it, even if the IT specifically affected is only indirectly threatened, for example, by actions by individuals.

Re subparagraph 22

The definition continues the previous Section 2(10) of the BSI Act with amendments due to the new general scheme. The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account. The provision will be amended in the foreseeable future, cf. Article 2.

Re subparagraph 23

The definition continues the previous Section 2(13).

Re subparagraph 24

The definition has been taken from Section 1(1)(3) of the BSI-KritisV.

Re subparagraph 25

The definition transposes Article 6(40) of the NIS 2 Directive.

Re subparagraph 26

The definition transposes Article 6(39) of the NIS 2 Directive.

Re subparagraph 27

The definition simplifies the many citations of the NIS 2 Directive in the BSI Act.

Re subparagraph 28

The definition transposes Article 6(28) of the NIS 2 Directive.

Re subparagraph 29

The definition transposes Article 6(29) of the NIS 2 Directive.

Re subparagraph 30

The definition transposes Article 6(33) of the NIS 2 Directive.

Re subparagraph 31

The definition continues the previous Section 2(8).

Re subparagraph 32

The definition continues the previous Section 2(8a).

Re subparagraph 33

The definition transposes Article 6(26) of the NIS 2 Directive.

Re subparagraph 34

The definition transposes Article 6(27) of the NIS 2 Directive.

Re subparagraph 35

The definition transposes Article 6(31) of the NIS 2 Directive. Data processing also includes, in particular, transport and storage.

Re subparagraph 36

The definition continues the previous Section 2(5).

Re subparagraph 37

The definition continues the previous Section 2(4). Terms are being consolidated/consequently changed – instead of federal authorities, federal administration entities. The adaptation widens the scope of the term – in view of the purpose of protecting the information security of federal networks and possible other government networks, the extension clarifies that it is not only federal authorities that can be connected to these networks.

Re subparagraph 38

The definition continues the previous Section 2(6) and at the same time serves to transpose Article 6(15) of the NIS 2 Directive.

Re subparagraph 39

The definition continues the previous Section 2(2), sentence 2.

Re subparagraph 40

The definition transposes Article 6(6) of the NIS 2 Directive.

Re subparagraph 41

The definition continues the previous Section 2(9b).

Re subparagraph 42

The definition transposes Article 6(21) of the NIS 2 Directive.

Re subparagraph 43

The definition transposes Article 6(24) of the NIS 2 Directive.

Re subparagraph 44

The definition transposes Article 6(25) of the NIS 2 Directive.

Re subparagraph 45

Reference is made to the statement of reasons relating to subparagraph 3.

Re subparagraph 46

The definition continues the previous Section 2(7).

Re Part 2 (The Federal Office)

Re Chapter 1 (Tasks and powers)

Re Section 3 (Tasks of the Federal Office)

With the implementation of the NIS 2 Directive, the list of tasks of the Federal Office will be expanded. In the light of Article 31(2), sentence 1 of the NIS 2 Directive, the Federal Office must decide on a voluntary basis, as it prioritises the performance of the tasks.

Re paragraph 1

Paragraph 1 continues the previous Section 3(1) and has been corrected by deleting the sentence 1. As ‘information technology security’ is a term defined in Section 2(39), which already contained the cleaned-up words, this was a circular argument.

Re subparagraph 1

The entry continues the previous Section 3(1), sentence 2, subparagraph 1.

Re subparagraph 2

The entry continues the previous Section 3(1), sentence 2, subparagraph 2.

Re subparagraph 3

The entry transpose Articles 14 and 15 of the NIS 2 Directive in the form of a task of the Federal Office.

Re subparagraph 4

The entry continues the previous Section 3(1), sentence 2, subparagraph 3.

Re subparagraph 5

The entry continues the previous Section 3(1), sentence 2, subparagraph 4.

Re subparagraph 6

The entry transpose Article 19 of the NIS 2 Directive in the form of a task of the Federal Office.

Re subparagraph 7

Here, tasks which are already assigned to the Federal Office under the Federal Implementation Plan and the 2030 Network Strategy are enshrined in law. The terminology is linked to Section 2(3) of the BDBOSG and clarifies the role of the Federal Office in the task of the Federal Agency for Public Safety Digital Radio (BDBOS): The Federal Office is in charge of organising information security in the interdepartmental communication infrastructures. In consultation with the relevant operators, it shall lay down information security requirements, examine plans and implementations from a safety point of view, including in the case of service providers and associated organisations, advise on alternative solutions and implementation, accompany acceptances from a safety point of view and manage safety management, in particular during the operational phase. Any deficiencies, risks or incidents identified shall be reported to the competent bodies.

Re subparagraph 8

The entry continues the previous Section 3(1), sentence 2, subparagraph 5.

Re subparagraph 9

The entry continues the previous Section 3(1), sentence 2, subparagraph 5a.

Re subparagraph 10

The entry continues the previous Section 3(1), sentence 2, subparagraph 6.

Re subparagraph 11

The entry continues the previous Section 3(1), sentence 2, subparagraph 7.

Re subparagraph 12

The entry continues the previous Section 3(1), sentence 2, subparagraph 8.

Re subparagraph 13

The entry continues the previous Section 3(1), sentence 2, subparagraph 9.

Re subparagraph 14

The entry continues the previous Section 3(1), sentence 2, subparagraph 10.

Re subparagraph 15

The entry continues the previous Section 3(1), sentence 2, subparagraph 11. There is a consolidation/extension of the scope to include federal administration entities. The extension is carried out for the purpose of ensuring a uniformly high level of security for all entities operating federal information technology. In addition, the provision of IT security products is complemented by the provision of IT security services. The need for IT security products; and -services, including the need for a CI authorisation, are identified by the Federal Office.

Re subparagraph 16

The entry continues the previous Section 3(1), sentence 2, subparagraph 12. ‘Bodies of the Federal Government’ will be maintained here, as extending it to all federal administration entities would result in significantly higher implementation costs, which would not be proportionate to the benefits.

Re subparagraph 17

The entry continues the previous Section 3(1), sentence 2, subparagraph 12a. Here there is a consolidation of the concept of ‘federal administration entities’. In addition to the obligation for futher entities to comply with the requirements of the Federal Office, the Federal Office’s task of providing advice and assistance should also be extended to these entities. This task is complemented by the provision of practical aids to make it clear that support from the Federal Office is not only limited to the care of individual entities, but also includes the provision of inter-entity tools to support all or more entities. In developing these tools (continued) the Federal Office takes account of practical experience.

Re subparagraph 18

The entry continues the previous Section 3(1), sentence 2, subparagraph 13. The possibility of the Federal Office providing mutual assistance to the Länder is not affected by the amendment to the previous Section 3(1) sentence 2 subparagraph 13.

Re subparagraph 19

The entry continues the previous Section 3(1), sentence 2, subparagraph 13a.

Re subparagraph 20

The entry continues the previous Section 3(1), sentence 2, subparagraph 14. A consolidation of terms into federal administrative entities is being carried out in order to avoid, a contrario, that entities which go beyond federal bodies are not covered. The possibility of the Federal Office providing mutual assistance to the Länder is not affected by the amendment to the previous Section 3(1) sentence 2 subparagraph 14.

Re subparagraph 21

The entry continues the previous Section 3(1), sentence 2, subparagraph 14a.

Re subparagraph 22

The entry continues the previous Section 3(1), sentence 2, subparagraph 15.

Re subparagraph 23

The entry continues the previous Section 3(1), sentence 2, subparagraph 16.

Re subparagraph 24

The entry continues the previous Section 3(1), sentence 2, subparagraph 17. A consequential amendment is made as a result of changes to the nomenclature: ‘operators of critical infrastructures’ are now uniformly defined as ‘operators of critical facilities’, and ‘digital service providers’ and ‘undertakings in the particular public interest’ in ‘particularly important entities’ and ‘important entities’.

Re subparagraph 25

The entry continues the previous Section 3(1), sentence 2, subparagraph 18. In addition, the incorrect reference to the former Section 5a instead of the former Section 5b shall be amended. The latter shall be continued by: Section 11.

Re subparagraph 26

The entry continues the previous Section 3(1), sentence 2, subparagraph 19.

Re subparagraph 27

The entry continues the previous Section 3(1), sentence 2, subparagraph 20.

Re subparagraph 28

This new task of the Federal Office is intended to transpose Article 10(8) of the NIS 2 Directive. This task is a specific legal arrangement for European mutual assistance which the Federal Office can exercise within the scope of its existing powers.

Re subparagraph 29

This new task of the Federal Office is to ensure the necessary coordination with BaFin. This is necessary in the light of sector-specific Regulation (EU) 2022/2554.

Re paragraph 2

Paragraph 2 continues the previous Section 3(2).

Re paragraph 3

Paragraph 3 continues the previous Section 3(3). It includes a consequential amendement due to the new term ‘critical facilities’.

Re Section 4 (Federal Financial Intelligence Unit for Information Technology Security)

Re paragraph 1

Paragraph 1 continues the previous Section 4(1). It contains a consolidation of ‘federal administration entities’.

Re paragraph 2

Paragraph 2 continues the previous Section 4(2). In subparagraph 1 the new term ‘vulnerability’ will be used. There is also a consolidation of the concept of ‘federal administration entities’ in: subparagraph 2. In addition, subparagraph 3 adds that the Federal Office must also provide the federal administration entities with recommendations relating specifically to the handling of the risks identified by the Federal Office.

Re paragraph 3

Paragraph 3 continues the previous Section 4(4).

Re Section 5 (General Reporting Centre for Information Technology Security)

Re paragraph 1

Section 5 Paragraph 1 continues the previous Section 4b(1). Adjustments are made to transpose Article 12(1), sentence 1 of the NIS 2 Directive (corresponding to Section 9a of the old version of the BSI Act).

Re paragraph 2

Section 5 Paragraph 2 continues the previous Section 4b(2). Addition to sentence 1 is made to transpose Article 30(1) of the NIS 2 Directive.

Re paragraph 3

Section 5 Paragraph 3 continues the previous Section 4b(3). The new subparagraph 5 transposes Article 30(2) of the NIS 2 Directive.

Re paragraph 4

Section 5 Paragraph 4 continues the previous Section 4b(4).

Re paragraph 5

Section 5 Paragraph 5 continues the previous Section 4b(5).

Re Section 6 (Information exchange)

The new provision transposes Article 29 of the NIS 2 Directive. The Federal Office makes it possible to exchange information on cyber threats (Section 2, subparagraph 6)), near misses (Section 2, subparagraph 1), vulnerabilities (Section 2, subparagraph 38)), t*echniques and procedures*, *indicators of compromise*, *adversarial tactics*, *threat-actor-specific information*, cybersecurity warnings and recommendations for the configuration of cybersecurity tools and for detecting cyberattacks. This exchange of information shall allow participating entities to have improved access to situational information and bi-directional exchange of information, and shall also allow participants to exchange with each other on observed threats at an early stage, thereby enhancing the cybersecurity and resilience of the entities.

By drawing up participation conditions, the Federal Office can regulate the organisational framework for the exchange of information in order to ensure the orderly and secure operation of the information exchange or the dedicated online portal.

In this context, for example, the handling of confidential information (e.g. compliance with the ‘Traffic Light Protocol’ or the use of encrypted email communications) may be regulated.

Re Section 7 (Control of federal communication technology, rights of access)

Re Paragraph 1 to Paragraph 7

The provision continues the previous Section 4a. Paragraph 4 shall be adapted in the context of the consolidation of the concepts of ‘federal administration entities’ provided for in this Act and the responsible federal information security management bodies established

by this Act, which also require a corresponding extension of the Federal Office's reporting obligations for the effective performance of their tasks. The operator refers to the entity concerned which operates the inspected communications technology of the Federal Government. The results of the inspections shall be communicated to the relevant entity management. A clarification of the facts is also added to prevent misunderstandings and errors. In addition, each inspected entity is free to submit its own comments on the Federal Office's inspection report to the bodies which received the Federal Office's inspection report, in particular to the department's own information security officer and its own technical and legal supervision. Paragraph 5 adds the power of the Federal Office to instruct the implementation of the proposals for improvement within a reasonable period of time. It transposes Article 32(4)(d) and (f) of the NIS 2 Directive. The power is an effective element for effective follow-up control when there is reason to do so. Examples may be when, for example, an inspection reveals a repeated significant failure to comply with information security management requirements. In order to remedy the shortcomings identified, the Federal Office shall provide advice and assistance from the Federal Office in accordance with: Section 3(1)(17). Editorial changes have also been made.

Re paragraph 8

Paragraph 8 transposes Article 35 of the NIS 2 Directive. Reference is made to the statement of reasons relating to Section 61(11).

Re paragraph 9

The aim of the new rule is to increase responsibility for implementation. So far, the inspections under the current Section 4a of the BSI Act have been without any tangible consequence for the inspected bodies. The report is submitted to the Budget Committee of the German Bundestag, as this means that it is reported to the body that has the resources to enable the elimination of irregularities. It is intended to replace the reporting obligation of the Federal Ministry of the Interior and Community to the Budget Committee of the German Bundestag on the results of the evaluation of the IT security of the Federal Administration's data centres by means of a high availability benchmark (Decision of the Budget Committee of the German Bundestag of 17 June 2015, Committee document 18(8)2134). There is a general obligation to report to the Committee of the Interior and Community of the German Bundestag according to Section 58(3) in any event, it includes reporting on the application of this provision.

Re Section 8 (Protection against malware and threats to federal communications technology)

Section 8 continues the previous Section 5.

Re paragraph 1

Paragraph 1 continues the previous Section 5(1). In sentence 3, the term is consolidated into 'federal administration entities', and this extension of the scope is made for the purpose of protecting the entire federal communications technology.

Re paragraph 2

Paragraph 2 continues the previous Section 5(2).

Re paragraph 3

Paragraph 3 continues the previous Section 5(2a).

Re paragraph 4

Paragraph 4 continues the previous Section 5(3).

Re paragraph 5

Paragraph 5 continues the previous Section 5(4).

Re paragraph 6

Paragraph 6 continues the previous Section 5(5). Both paragraphs 6 and 7 refer to data within the meaning of paragraph 1 which are subject to the protection of telecommunications secrecy and the protection of personal data and for which further use in accordance with paragraph 4 is required. Since in paragraph 4 the use of the data may only be ordered by an official of the Federal Office with the capacity to hold judicial office, this is also supplemented in paragraph 6.

Re paragraph 7

Paragraph 7 continues the previous Section 5(6). The possibility is added for the Federal Office to transmit the personal data used in accordance with paragraph 4 to the federal administration entities for whose protection the data have been technically collected, in so far as this is necessary for the use referred to in paragraph 4 or for the prevention of other significant threats to information security. This ensures that the federal entities receive all relevant information to ensure the protection of the federal communications technology.

Re paragraph 8

Paragraph 8 continues the previous Section 5(7).

Re paragraph 9

Paragraph 9 continues the previous Section 5(8). The reference to the ‘Council of IT Commissioners of the Federal Government is replaced by ‘departments’ in order to be able to regulate the committee structure sub-legally.

Re paragraph 10

Paragraph 10 continues the previous Section 5(9).

Re paragraph 11

Paragraph 11 continues the previous Section 5(10).

Re Section 9 (Processing of logging data from federal communications technology)

Section 9 continues the previous Section 5a. The amended heading reflects the consolidation of terms and the reference to the content of: Section 8. The term is consolidated into ‘federal administration entities’. The extension of the scope is made for the purpose of protecting the entire federal communications technology.

Re Section 10 (Ordering of measures to prevent or remedy security incidents)

The new provision transposes Article 32(4)(b) and (5) of the NIS 2 Directive vis-à-vis central government entities in response to acute security incidents; in order to ensure a coherent regulatory regime and effective operational incident management, the powers set out in: Section 29 are also extended to the other federal administration entities. If the Federal Office identifies a danger or the existence of a security incident, it shall draw the at-

tention of the federal administration bodies to the measures it considers necessary to prevent or remedy it. If the institutions do not implement these measures within a reasonable period of time, even though the Federal Office considers that they are necessary, it may instruct the institutions to implement them. It will normally consult the entities in advance. In the event of imminent danger, it may also issue the order without giving the institutions the opportunity to comment beforehand. When issuing instructions, the Federal Office takes into account potential effects on third parties, such as customers or service providers. The instructions issued by the Federal Office to the federal administration entities are addressed to the respective head of the entity. Possible examples of instructions from the Federal Office may be, depending on the situation, on the basis of a case-by-case factual and legal assessment: Transfer of systems or data to the Federal Office for evaluation; increased logging for anomalie detection; Extension of retention periods; Preventing data deletion; Installation of a network sensor of the Federal Office for detection; An obligation to inform or not inform employees, service providers, clients and partners about certain facts; Non-network disconnection to ensure the evaluation of attacker behaviour; in extreme cases, disconnection. In accordance with the different roles in the supervisory structure, reporting to the Federal Office as the operational supervisory authority and to the information security officer of the department as competent technical supervision is also planned.

Re Section 11 (Restoring the security or functioning of information technology systems in exceptional cases)

Section 11 continues the previous Section 5b.

Re paragraph 1

Paragraph 1 continues the previous Section 5b(1). There is a consequential change due to new categories of entities, as well as an adaptation to transpose Article 11(1)(d) of the NIS 2 Directive. The term is also consolidated into ‘federal administration entities’.

Re paragraph 2

Paragraph 2 continues the previous Section 5b(2).

Re paragraph 3

Paragraph 3 continues the previous Section 5b(3). An editorial amendment has been made, as according to Article 4(2) of the General Data Protection Regulation, the concept of processing already includes collection.

Re paragraph 4

Paragraph 4 continues the previous Section 5b(4). The term ‘information’ covers any knowledge relating to the entity concerned of which the Federal Office becomes aware in the course of its services under Section 11.

Re paragraph 5

Paragraph 5 continues the previous Section 5b(5).

Re paragraph 6

Paragraph 6 continues the previous Section 5b(6).

Re paragraph 7

Paragraph 7 continues the previous Section 5b(7).

Re paragraph 8

Paragraph 8 continues the previous Section 5b(8).

Re Section 12 (Inventory data disclosure)

Section 12 continues the previous Section 5c. The terms have been adapted to the new category designations.

Re Section 13 (Warnings)

Section 13 continues the previous Section 7.

Re paragraph 1

Paragraph 1 continues the previous Section 7(1). The new point 1(e) transposes Articles 32(4)(a) and 33(4) of the NIS2 Directive.

Re paragraph 2

Paragraph 2 continues the previous Section 7(1a).

Re paragraph 3

Paragraph 3 continues the previous Section 7(2). The provision is supplemented by a rule on the archiving of warnings. The background is the decision of the Federal Constitutional Court (BVerfG) of 21 March 2018 (– 1 BvF 1/13 –) on Section 40 LFGB. There was no statutory provision in the LFGB on the temporal limitation of the dissemination of information. This is incompatible with the principle of proportionality, since the lapse of time after the publication of the infringement of fundamental rights is disproportionate, on the one hand, to the detriment of the manufacturer and, on the other hand, to the purpose of the warning.

The nature and extent of any claims for compensation shall be determined in accordance with the general principles of State liability law.

Re Section 14 (Security investigation in information technology, request for information)

Section 14 continues the previous Section 7a.

Re paragraph 1

Paragraph 1 continues the previous Section 7a(1).

Re paragraph 2

Paragraph 2 continues the previous Section 7a(2).

Re paragraph 3

Paragraph 3 continues the previous Section 7a(3).

Re paragraph 4

Paragraph 4 continues the previous Section 7a(4). The addition made is necessary in order to allow and facilitate exchanges with third parties (such as other supervisory authorities) where, for example, only categories of product types and vulnerabilities found are

concerned, which are to be passed on without any specific reference to the manufacturer/product. Given that in this case the intensity of intervention vis-à-vis the manufacturers of the products and systems under investigation is considered to be very low in the absence of reference, a prior opinion would make it unnecessarily difficult to pass on critical vulnerabilities to third parties (such as other supervisory authorities).

Re paragraph 5

Paragraph 5 continues the previous Section 7a(5).

Re Section 15 (Detection of attack methods and security risks for network and IT security)

Section 15 continues the previous Section 7b and at the same time serves to transpose the NIS 2 Directive. The so-called vulnerability scans are a supervisory measure taken by the BSI to ensure that the addressed federal administration bodies and the particularly important and important institutions do not operate information technology systems that are exposed to a known vulnerability or other known security risk. The right to query referred to in paragraph 1 therefore corresponds to an information obligation under paragraph 2 as the sole purpose of data processing. Section 15 does not, however, authorise the detection of particularly sensitive, unknown vulnerabilities (also: zero-day vulnerabilities).

Re paragraph 1

Paragraph 1 continues the previous Section 7b(1) in line with the explanatory memorandum to the IT-SIG 2.0. The amendments are intended primarily to transpose Article 11(3)(e), Article 32(2)(d) and Article 33(2)(c) of the NIS 2 Directive, which consider the implementation of vulnerability scans of key and essential entities to be a mandatory task of CSIRTs and supervisory action. For example, faulty configurations may be considered as other already known security risks within the meaning of sentence 1. The detection of vulnerabilities is possible in addition to port scans using other web-page/domain-based methods. As technological progress may change the type of vulnerability scans, a formulation open to development had to be chosen. In accordance with the Directive, the rules also allow scanning of, for example, the systems operated by IT service providers for the entity. The chosen term ‘query’ refers to an open, non-intrusive type of IT query to the publicly accessible interfaces, which is in principle provided for in the technical specification of the interface. It is used exclusively for the detection of system characteristics and excludes any influence on the system. When vulnerabilities become known in the specification or implementation of an interface, queries to the publicly accessible interfaces may be carried out in a way that makes it possible to verify that the systems consulted contain this type of vulnerability. It was also necessary to adapt the scheme to the new categories of entities under the NIS 2 Directive. To harmonise terminology across Europe, the term ‘vulnerability’ within the meaning of Article 6(15) of the NIS 2 Directive is used instead of ‘security gap’, without this entailing any change in content. The deletion of Section 7b(2) is a consequential amendment to the adaptation of the conditions laid down in paragraph 1, which, in return for lowering the intervention threshold, provides for a limitation of the possible use of detected, known shortcomings. The Federal Office can thus examine the information technology systems of the above-mentioned entities for the existence of such weaknesses, which are not yet necessarily known to the public, but in any event to informed professionals. On the one hand, it must not use the standard to explore and exploit unknown new vulnerabilities (zero-day exploits) and, on the other hand, it may begin to compare and investigate known vulnerabilities in order to inform data subjects, without the vulnerabilities having first been made known to the general public.

Re paragraph 2

Paragraph 2 continues the previous Section 7b(3). Neither Section 8(7) nor Section 3(1)(2) allows the specific information on the vulnerabilities detected pursuant to paragraph 1

to be passed on. Paragraph 2 shall be regarded as an exhaustive provision in this respect. In order to close detected vulnerabilities as soon as possible, the Federal Office's obligation to provide information in the case of relevant federal administration entities must be extended to the information security officers of the entity and department (technical supervision).

For the purpose of the situational picture, the Federal Office may prepare, share and publish information extracted from the vulnerability scans (e.g. on the number and type of entities affected or the type of vulnerabilities).

Re paragraph 3

Paragraph 3 continues the previous Section 7 b(3) sentence 4.

Re paragraph 4

Paragraph 4 continues the previous Section 7b(1) sentences 2 and 3, but exempts the Federal Office from the burdensome maintenance of the so-called 'white list', which also covers IP addresses of information technology systems that have not been scanned. The resulting failure to carry out prior checking is compensated for by the fact that the BfDI can now, by means of the possibility of issuing a request, verify that the IT systems actually scanned by the Federal Office are also assigned to a body of federal administration, a particularly important body or an important body.

Compared to Section 7b paragraph 1 the previous restriction to internet protocol addresses is also deleted. Instead, it also includes other systems, which, in addition to internet protocol addresses, may include, for example, domains to be scanned. In the case of vulnerability scans, it is not intended to interfere with the fundamental right to informational self-determination, depending on the possible weakness, under art. 2, paragraph 1 in conjunction with art. 1, paragraph 1 GG and telecommunications secrecy from art. 10 paragraph 1 GG, the Federal Commissioner for Data Protection and Freedom of Information may, in the context of his or her independence, exercise a means of supervision for the data subjects.

Re paragraph 5

Paragraph 5 continues the previous Section 7b(4).

Re Section 16 (Ordering measures by the Federal Office against telecommunication services providers)

Section 16 continues the previous Section 7c.

Re paragraph 1

Paragraph 1 continues the previous Section 7c(1). As the term 'service provider' is now used in the law with different meanings due to the implementation of the NIS 2 Directive, it was necessary to adapt the legal definition only for the purposes of this provision. The word 'concrete' in the previous provision has been deleted by way of drafting clarification.

Re paragraph 2

Paragraph 2 continues the previous Section 7c(2). In subparagraph 1, a consequential amendment is made due to the new category designations.

Re paragraph 3

Paragraph 3 continues the previous Section 7c(3).

Re paragraph 4

Paragraph 4 continues the previous Section 7c(4).

Re Section 17 (Ordering measures by the Federal Office against digital service providers)

Section 17 continues the previous Section 7d. The words ‘reasoned’ and ‘concrete’ in the previous provision in the sentence 1 have been deleted by way of drafting clarification.

Re Section 18 (Ordering measures by the Federal Office against manufacturers of ICT products)

Section 18 continues the previous Section 8b(6). Federal institutions – in particular those which are federal IT service providers – may also be manufacturers, provided that they produce ICT products.

Re Section 19 (Provision of IT security products)

Section 19 continues Section 8(3), sentences 1-3. There is a consolidation of terms into ‘federal administration entities’ in order to broaden the scope of application for the protection of the entire federal communications technology, giving concrete expression to the role of the Federal Office with regard to Section 3(1) subparagraph 15. Attention is also drawn to compliance with the Federal Budget Regulation.

Re Chapter 2 (Data processing)

Re Section 20 (Processing of personal data)

Section 20 continues the previous Section 3a.

Re Section 21 (Restriction of data subject rights)

Section 21 continues the previous Section 6.

Re Section 22 (Duty to provide information when collecting personal data)

Section 22 continues the previous Section 6a.

Re Section 23 (Right of access by the data subject)

Section 23 continues the previous Section 6b.

Re Section 24 (Right to rectification)

Section 24 continues the previous Section 6c.

Re Section 25 (Right to erasure)

Section 25 continues the previous Section 6d.

Re Section 26 (Right to restriction of processing)

Section 26 continues the previous Section 6e.

Re Section 27 (Right to object)

Section 27 continues the previous Section 6f.

Re Part 3 (Security in the information technology of entities

Re Chapter 1 (Scope of application)

Re Section 28 (Particularly important and important entities)

Section 28 transposes Article 3 of NIS 2 Directive.

Re paragraph 1

Paragraph 1 defines particularly important entities. The inclusion of legally dependent organisational units of a regional authority ensures that in-house operations and Land operations that provide corresponding services in accordance with the definitions of institutions can be adequately addressed, even if they are not legal entities or natural persons. In order to improve readability, the size thresholds for the number of employees and annual turnover referred to in Commission Recommendation 2003/361 EC are in principle defined in this Act.

In so far as this paragraph indicates categories of entities without an explicit indication of the number of employees, the annual turnover or the annual balance sheet total, these definitions apply in each case irrespective of the size of the undertaking.

Re subparagraph 1

Subparagraph 1 transposes Article 3(1)(f) of the NIS 2 Directive, according to which critical entities or operators of critical facilities are also deemed to be particularly important entities within the meaning of this Act in accordance with the CER Directive.

Re subparagraph 2

Subparagraph 2 transposes Article 3(1)(b) of the NIS 2 Directive.

Re subparagraph 3

Subparagraph 3 transposes Article 3(1)(c) of the NIS 2 Directive.

Re subparagraph 4

Subparagraph 4 transposes Article 3(1)(a) of the NIS 2 Directive.

Re paragraph 2

Paragraph 2 defines important entities and transposes Article 3(2) of the NIS 2 Directive. The above references in the explanatory memorandum to paragraph 1 shall apply accordingly.

Re paragraph 3

When determining the relevant employee numbers and turnover, only those parts of the entity that are actually active in the area of the definitions of the entity categories listed in Annexes 1 and 2 are to be included; cross-divisional tasks such as personnel, accounting, etc. are to be taken into account on a pro rata basis. This ensures that entities which, in total, exceed the size threshold for the number of employees, annual turnover or annual balance sheet total, but whose main business activity does not fall within an entity cate-

gory in accordance with Annex 1 or 2 to this Act, are not recorded in a disproportionate manner.

For the purposes of determining the number of employees, annual turnover and annual balance sheet total, Recommendation 2003/361/EC shall apply to entities which are not legally independent organisational units of a local authority, with the exception of Article 3(4) of the Recommendation. According to that provision, the data refer in principle to the entity's most recent accounts and are calculated on an annual basis, cf. Article 4(1) of the Annex to Recommendation 2003/361/EC. This means that, in particular, seasonal overruns of the threshold are not decisive in terms of the number of employees within one year. Furthermore, an entity loses the status of a medium-sized enterprise, a small enterprise or a micro-enterprise only if it exceeds or falls short of the size threshold for two consecutive financial years, cf. Article 4(2) of the Annex to Recommendation 2003/361/EC. As a result, individual economically successful or unsuccessful financial years do not in themselves lead to the recording as a particularly important or important entity.

The data of partner or related enterprises within the meaning of Recommendation 2003/361/EC are not to be added if, taking into account the legal, economic and factual circumstances, the enterprise in question exercises decisive influence over the nature and operation of the information technology systems, components and processes that the enterprise uses to provide its services. There is a decisive influence on the design and operation of the information technology systems, components and processes, in particular where fundamental decisions on the acquisition, operation and configuration of the information technology systems, components and processes can be taken by the facility under its own responsibility. For example, this should normally be denied if the information technology systems, components and processes are operated entirely by a parent company and the entity itself cannot in fact exert any influence on the aforementioned properties. However, decisive influence is regularly present when the information technology systems, components and processes are operated on behalf of a service provider, since contractual arrangements can exercise decisive influence over the aforementioned properties. This ensures that partner enterprises or subsidiaries which individually do not meet or exceed the foreseen thresholds for the number of employees, annual turnover and annual balance sheet total can only be considered as particularly important entities in those cases if they do not exercise decisive influence over their own information technology systems, components and processes, for example because they are operated by a partner enterprise.

Re paragraph 4

Paragraph 4 provides for exceptions for certain categories of entities regulated by special law. Paragraph 4 continues the previous Section 8d(2). The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account. For operators of public telecommunications networks, energy supply networks and energy installations, the current special legislation with a corresponding competence of the Federal Network Agency and IT security catalogues prepared by the Federal Network Agency for this purpose will continue.

Paragraph 4, sentence 1, excludes from the above-mentioned BSIG rules all entities which operate an installation covered by the TKG or EnWG. The aim is to avoid double regulation by BNetzA and BSI: in this case, the NIS 2 Directive is fully implemented by the provisions of the TKG and the EnWG.

At the same time, this derogation is not intended to limit the applicability of the BSIG, and thus the BSI's competence, to other sectors. For example, an example could be the case in which a facility simultaneously includes a water plant under point 5.1.1 of Annex 1 and

an electricity power plant under point 1.1.4 of Annex 1, whose IT systems are in principle operated separately, but both interfaces with a common monitoring system.

In this case, paragraph 4 sentences 2 and 3 provide for a corresponding exception, which would extend to the IT of the waterworks, including its interface with the monitoring system. The exception therefore covers all IT relevant to the activities in these sectors – or the operation of the relevant critical facility. This is therefore again subject to the requirements of the BSIG, so that, in particular, appropriate industry-specific safety standards under Section 30(8) and (9) can also be applied.

On the other hand, the exception does not cover corporate IT which is not relevant to the activity in these other sectors (e.g. office IT without interfaces to critical facilities).

Thus, in theory, parts of IT may also be subject to the supervision of both BNetzA and BSI, i.e. when this is relevant to the activity in different sectors.

As a result, all IT systems are subject to regulation (including the requirement of Article 21(1) of the NIS 2 Directive).

Re paragraph 5

Re subparagraph 1

In implementation of recital 28 of the NIS 2 Directive, Regulation (EU) 2022/2554 (DORA Regulation) applies to financial entities as lex specialis. Therefore, these companies are exempted from the obligations set out in this paragraph.

Re subparagraph 2

Subparagraph 2 continues the previous Section 8d(2)(3) and (3)(3).

Re paragraph 6

Paragraph 6 stipulates that operators of critical facilities whose service recipients are already subject to Regulation (EU) 2022/2554 (DORA) and are required to report under this Regulation are not subject to a further reporting obligation under Section 32 of this Act. Voluntary notifications under Section 5 are still possible.

Re paragraph 7

Paragraph 7 defines operators of critical facilities.

Re paragraph 8

This opening clause allows the Länder, under their own responsibility, to exclude from the scope of this law entities which are 100 % owned by Länder and municipalities and have been set up for the purpose of providing services to administrations on a public service mission. Finally, it is necessary that the entity be the subject of a NIS 2 implementation by the country concerned comparable to the provisions of this Act and that the country also makes use of this opening clause by referring to the opening clause. The latter is intended to ensure that no entities which are to be regulated by the Federal Republic of Germany in implementation of the NIS 2 Directive are left free of regulation.

The scope of Section 28 covers only entities operating economically. In that regard, only legally independent organisational units of local authorities and legal persons which are economically active can be excluded by means of that opening clause.

Re Section 29 (Federal Administration entities)

Section 29 includes federal administrative entities as a category in the regulatory regime established with the implementation of the NIS 2 Directive. In many federal administration entities, there is a deficit in the implementation of own protection measures in the area of information security. The current governance instruments on a predominantly sub-statutory basis (such as the federal implementation plan) have not proved to be sufficiently effective to achieve a comprehensive and effective increase in the level of safety. Against the backdrop of the current geopolitical developments (‘turning point’), the threat situation has once again intensified, further increasing the risk of governmental entities being restricted in their ability to act by threats from cyberspace. The implementation of the NIS 2 Directive is therefore accompanied by these and other provisions with further rules on federal administration going beyond the mere implementation of the NIS2 Directive. In order to achieve a common, coherent and manageable regime at federal level, also in the context of the interconnectedness and consolidation of IT as a whole, requirements are formulated under national responsibility which are based on the content of those for particularly important entities.

Re paragraph 1

Paragraph 1 defines the category of federal administrative entities within the meaning of this Act. In the light of the protective purpose of the Federal Government’s information security and for the purpose of consolidating the concepts, the definition is fundamentally based on the scope of the former Section 8(1) and the scope of the Federal Government Implementation Plan, which has already established the concept of federal administrative entities. The administration of the Bundestag and the Secretariat of the Bundesrat are included as federal authorities in suparagraph 1. It does not include the Versorgungsanstalt der deutschen Bühnen (the German Theatre Pension Institution), the Versorgungsanstalt der deutschen Kulturorchester (the German Cultural Orchestras Pension Institution) and the Versorgungsanstalt der bevollmächtigten Bezirksschornsteinfeger (the care agency of authorised district chimney sweeps), which are administered by a Land authority. Subparagraph 3 maintains the existing ‘opt-in’ requirement. In principle, further direct bodies, institutions and foundations governed by public law, as well as their association, should be ordered if the entity concerned performs administrative tasks under public law and there could be a discernible adverse impact on the Federal Government’s information security as a result of a failure to order the entity. Apparent adverse effects on the Federal Government’s information security may arise, in particular, if the entity poses a potential risk of interconnection for other federal entities; for example, if the entity is connected to the federal networks or uses services of the Federal Government’s IT consolidation. In order to be able to properly assess the potential adverse effects, the order is made by the Federal Office in agreement with the relevant department. In addition, the Federal Administration’s IT service providers organised under public law are explicitly included in the scope, i.e. the association of the Federal IT service providers (VITD) with the exception of BWI GmbH, which is governed by private law, and the Federal Employment Agency and Deutsche Rentenversicherung, regulated as KRITIS, as social security institutions.

Re paragraph 2

Paragraph 2 serves as a general clause to extend the scope in principle to entities of the federal administration which are not themselves particularly important or important entities, and to lay down derogations for federal administration entities from the rules applicable to (particularly) important entities.

For entities of the federal administration, the rules for particularly important entities apply, provided that there are no derogations for federal administration entities. In other words, the following rules apply to particularly important entities: Sections 6, 12, 13 (1), subparagraph 1(e), Sections 30, 32, 33, 35, 36, 37, 56 and 59where Section 30 is fulfilled by com-

plying with Section 44(2) and applies only to the Federal Chancellery and the Federal Ministries, without the respective subordinate business area. Section 44(1) shall apply to all other entities of the federal administration, which continues the previous Section 8(1). The following rules for particularly important or important entities shall not apply: Sections 38, 40 (3), 61 and 6565, as the following derogations apply instead: Seections 4, 7, 10, 43 paragraphs 1, 2, 4 and 5.

Re paragraph 3

Paragraph 3 defines the exception in the field of defence and national security in the NIS 2 Directive. Furthermore, according to its Recital 8, the NIS 2 Directive does not apply to diplomatic and consular representations of Member States in third countries. Therefore, in order to take into account the specificities of the External Action Service, the Federal Foreign Office will take its own measures in its portfolio to implement the objectives of the Directive.

Re Chapter 2 (Risk management, reporting, registration, demonstration and information obligations)

Re Section 30 (Risk management measures of particular importance and important entities)

Section 30 transposes Article 21 of the NIS 2 Directive. For federal administrative entities, Section 30 is transposed by Section 44.

Re paragraph 1

Paragraph 1 transposes Article 21(1) and (4) NIS 2 Directive. While, in the field of cybersecurity measures, the BSIG has so far focused on the information technology systems, components and processes that are relevant for the functioning of the critical infrastructure for critical infrastructure operators, in future, all information technology systems, components and processes used by the entity to provide its services will have to be taken into account as a result of the implementation of the NIS 2 Directive. The term ‘provision of their services’ is defined broadly and in particular not to be confused with the provision of (critical) utilities. Rather, the services referred to here are all the activities of the entity using IT systems, including, for example, office IT or other IT systems operated by the entity.

Risks are the potential for losses or disruptions caused by an incident expressed as a combination of the magnitude of such loss or disruption and the probability of the occurrence of the incident. Paragraph 1 clarifies that only appropriate, proportionate and effective measures are to be taken by the entity. In terms of proportionality, particular account shall be taken of the risk exposure, the size of the entity, the compliance costs and the likelihood and severity of incidents, as well as their societal and economic impact. This is for the purpose of transposing Article 21(1), subparagraph 2, NIS 2 Directive. In order not to impose a disproportionate financial and administrative burden on particularly important and important entities, those risk management measures shall be proportionate to the risks to which the network and information system concerned is exposed. This will take into account, inter alia, the costs of implementation and the size of the institution. The assessment of appropriateness and proportionality may also take into account whether it is an important entity, a particularly important entity compared to an essential entity or an operator of a critical installation, as different levels of risk exposure can in principle be assumed in those entities categories. ‘Risk’ means the potential for loss or disruption caused by an incident expressed as a combination of the magnitude of such loss or disruption and the probability of the occurrence of the incident. When assessing the appropriateness and proportionality of the measures in question, it may also be taken into account whether this protects services which have a compelling operational link with the goods or services which have led to the assignment to one of the types of facilities defined in Appendix 1 or 2.

Similarly to accountability under Article 5(2) of Regulation (EU) 2016/679 (General Data Protection Regulation), institutions are required to adequately document the implementation and compliance of measures. This obligation ensures that entities can submit corresponding verification documents to the Federal Office following requests for verification by the Federal Office pursuant to Section 61(3). Such documentation may include, for example: internal guidelines, instructions, checklists, staff training, agreements, fact sheets, etc., but also audit reports, certifications or audits.

Re paragraph 2

Paragraph 2 transposes Article 21(2) of the NIS 2 Directive. The requirements set out here, in particular in the area of supply chain security, may also include the carrying out of External Attack Surface (EAS) Scans. With the requirement in point 2, the technical term '*incident response*'indicated.

The term 'cyber hygiene' within the meaning of the NIS 2 Directive defines various basic processes and approaches that can generally lead to an improvement of an entity's level of cybersecurity. This includes, for example, patch management, secure password arrangements, administrator-level access restrictions, network segmentation, and data backup and backup concepts. It also includes general information and training activities to raise staff awareness of the risks associated with ICT products.

Measures relating to supply chain security include, for example, contractual agreements with suppliers and service providers on risk management measures, cybersecurity incident management, patch management, and the consideration of Federal Office recommendations in relation to their products and services. This may also include encouraging suppliers and service providers to comply with fundamental principles such as Security by Design or Security by Default. When considering appropriate measures pursuant to paragraph 4, subparagraph 4, the entity shall take into account the specific vulnerabilities of each direct supplier and service provider, as well as the overall quality of the products and cybersecurity practices of their suppliers and service providers, including the security of their development processes. When considering appropriate measures under sentence 1, entities shall take into account the results of the coordinated risk assessments of critical supply chains carried out in accordance with Article 22(1) of the NIS 2 Directive.

Re paragraph 3

Paragraph 3 transposes Article 21(5)(1) of the NIS 2 Directive.

Re paragraph 4

Paragraph 4 transposes Article 21(5)(2) of the NIS 2 Directive. Where the European Commission adopts an implementing act pursuant to Article 24(2) of the NIS 2 Directive, its provisions on the use of certified ICT products, ICT services and ICT processes shall take precedence over those set out in sentence 1.

Re paragraph 5

In order to take due account of the threat situation, the Federal Office must be able to require the implementation of appropriate measures in addition to any measures adopted by the European Commission.

Re paragraph 6

Paragraph 6 transposes Article 24 of the NIS 2 Directive. Article 24(2) of the NIS 2 Directive also empowers the EU Commission to adopt delegated acts under Article 290 TFEU, which may also require the mandatory use of certified products, services or processes in accordance with European schemes. These delegated acts shall take precedence accord-

ingly over a statutory ordinance issued by the Federal Ministry of the Interior and Community pursuant to paragraph 6 of this Regulation.

Before adopting such a statutory ordinance, the Federal Ministry of the Interior and Community and the other departments involved must ensure that appropriate certification schemes are in place and that products, services or processes certified according to these certified products, services or processes are sufficiently available on the market to avoid downstream problems caused by shortages or difficulties in supply.

Re paragraph 7

Paragraph 7 goes beyond the mere 1:1 transposition of the NIS 2 Directive. As the implementation of Article 29 of the NIS 2 Directive is implemented through the Federal Office's Central Exchange Platform (BISP), this paragraph 7 aims to ensure bi-directional exchange.

Re paragraph 8

The Federal Government considers that the possibility for KRITIS operators to propose industry-specific safety standards (B3S) to meet the legal requirements, which are then assessed by the Federal Office in consultation with the Federal Office for Civil Protection and Disaster Assistance and the competent Federal supervisory authority, has proved to be very effective in implementing the NIS 1 Directive. Since the evaluation of the KRITIS-related components of the IT Security Act 2.0 has also unanimously encouraged the introduction of a similar procedure from industry, paragraph 9 introduces a similar regime for particularly important entities. When developing sector-specific safety standards by operators of critical installations and their industry associations in order to meet the demonstration requirements under: Section 39(1) it may be useful to limit the measures to those information technology systems, components and processes relevant to the functionality of the critical installations. However, such an industry-specific safety standard is then only for the purpose of demonstrating the requirements set out in: Section 39(1) by operators of critical installations. Provided that the Federal Office: Section 61(3) Evidence from critical entities that are at the same time operators of critical installations shall be required by the entity to provide further evidence for those information technology systems, components and processes that the entity uses to provide its services but which are not covered by the industry-specific safety standard.

In cases where there is no competent federal supervisory authority in the health sector, consultation with the Federal Ministry of Health shall be established when establishing the sector-specific safety standards. The aim is to ensure legal harmonisation with the requirements of Book V of the Social Code.

Re paragraph 9

Paragraph 9 continues the previous Section 8a(2).

Re Section 31 (Specific requirements for risk management measures of operators of critical installations)

Section 31 defines additional requirements for operators of critical installations.

Re paragraph 1

Paragraph 1 provides that, in the case of measures to be implemented by operators of critical installations in accordance with Section 30, in relation to supply-related information technology systems, components and processes, there are higher requirements compared to the requirements for particularly important entities for other non-supply-related areas. Operators of critical installations shall ensure, within their entity, a further increased

level of safety for the information technology systems, components and processes that are relevant for the functioning of the critical installations they operate vis-à-vis important and critical entities. As regards the particularly serious social and economic impact of an adverse effect, the relevance of critical installations for the supply of critical installations to the population is a particular indication of the economic adequacy of the application of protective measures. Therefore, measures which increase the resilience of the installation in order to ensure security of supply for the population at the highest possible level, including in relation to usual realistic threat scenarios in accordance with the current situation reports and assessments of the Federal Office, are in principle considered appropriate in relation to the required effort.

With reference to paragraph 2, the paragraph makes no statement on the technical appropriateness of a measure to minimise a risk, but specifies that, in the case of critical installations, a fundamental balancing exercise must be made in favour of applying a measure against considerations of economic efficiency. In contrast to important and particularly important institutions, the balancing exercise is even more important in favour of the safety of the plant's functioning. The balancing exercise relates to measures for the information technology systems, components and processes in the installation that are necessary for it to function, and therefore not to the entire facility.

Re paragraph 2

Paragraph 2 requires operators of critical installations to use intrusion detection systems.

Re Section 32 (Reporting obligations)

Re paragraph 1

Paragraph 1 transposes the Article 23(4), sentence 1 of the NIS 2 Directive. 'Knowledge' means that a staff member of the institution becomes aware of a significant incident within his or her working hours. The Federal Office shall make it possible to communicate in English as far as possible.

Where a reportable security incident affects several entities within a group of companies, and if one or more standardised, possibly also cross-sector contact points have been designated for these entities within the group of companies, the other entities within the group of companies affected by the incident may also be indicated directly in the reporting form when submitting an incident report in accordance with paragraph 1. This makes it possible to avoid multiple reporting within a group of companies on the same incident with the aim of minimising red tape. Within the group, however, it must be ensured in this case that the contact points designated within the group can also provide information or designate a contact person on site or facility-specific queries from the Federal Office, for example on the impact of the security incident.

The reporting unit to be set up on the basis of this provision can be expanded in the future to also reflect further reporting obligations, such as under Regulation (EU) 2022/2554.

Re paragraph 2

Paragraph 2 transposes Article 23(4), sentence 1, point (e) of the NIS 2 Directive.

Re paragraph 3

Paragraph 3 requires KRITIS operators to continue to provide further information in relation to the assets concerned, the critical service concerned and the impact of the incident on that service when complying with incident reporting.

Re paragraph 4

In order to ensure an efficient and bureaucratic notification procedure, the Federal Office shall lay down details of the notification procedure after consulting the operators and business associations concerned. Where the European Commission adopts an implementing act in accordance with Article 23(11)(1) of the NIS 2 Directive specifying the type of information, format or procedure of the notifications, these requirements shall be complied with.

Re paragraph 6

Paragraph 6 contains a reference to the Federal Office's feedback to reporting entities according to Section 36(1). This does not imply that the notifying institution has a legal right to receive support from the Federal Office. The Federal Office continuously develops its support and information services for the reporting institutions and the economy as a whole, within the limits of its possibilities and in the performance of its existing statutory tasks, in an appropriate manner.

Re Section 33 (Registration obligation)

Section 33 implements Article 3(3) of the NIS 2 Directive. In Section 43(4) it is also stipulated that registration with institutions is the responsibility of the head of the institution.

The designation of the federal supervisory authorities responsible for the activity on the basis of which registration takes place is necessary in order for the Federal Office to meet the requirements of participation and information in relation to those authorities.

Re paragraph 1

Paragraph 1 transposes Article 3(4)(2), sentence 1 of the NIS 2 Directive. According to Section 29 accordingly, the obligation to register also applies to federal administrative bodies to the same extent. This will be clarified in Section 43(4), sentence 1.

For group structures it may be useful, from an efficiency point of view, to designate one or more single contact points within the group for more than one entity. This is in principle possible, provided that it is ensured that the information referred to in paragraph 1 is available for all registration obligations and the designated superior contact point within the group can also provide information on site-specific or facility-specific queries from the Federal Office.

Re subparagraph 1

Subparagraph 1 transposes point (a) of of Article 3(4)(1) of the NIS 2 Directive. The requirement is extended to include the trade register number, as the company alone is not clear.

Re subparagraph 2

Subparagraph 2 transposes point (b) of Article 3(4)(1) of the NIS 2 Directive.

Re subparagraph 3

Subparagraph 3 transposes point (c) of Article 3(4)(1) of the NIS 2 Directive.

Re subparagraph 4

Subparagraph 4 transposes point (d) of Article 3(4)(1) of the NIS 2 Directive.

Re subparagraph 5

The purpose of the provision is to facilitate cooperation with the competent supervisory authorities on a case-by-case basis.

Re paragraph 2

Paragraph 3 provides for additional information to be provided by operators of critical installations upon registration. Paragraph 3 continues the previous Section 8b(3), sentences 1 and 3. It is added that operators of critical installations must also submit the supply ratios of their critical installation.

Re paragraph 3

Paragraph 3 provides that entities and service providers may also be registered by the Federal Office itself if an entity or provider fails to comply with its obligation to register. Paragraph 3 continues the previous sentence 2 of Section 8b(3) and extends it to the types of establishments referred to here.

Re paragraph 4

Paragraph 4 continues the previous Section 8b(3a). The security interests referred to here or overriding security interests relate to the corresponding interests of the Federal Republic of Germany. The mere fact that commercial and business secrets of the companies involved do not justify a lawful refusal to submit the information.

Re paragraph 5

Paragraph 5 transposes sentence 2 of Article 3(4)(2) of the NIS 2 Directive.

Re paragraph 6

In order to make uniform registration processes possible and thus to make the administrative burden for the Federal Office and the compliance costs for the business sector efficient, the Federal Office is to lay down uniform rules on the registration procedure.

Re Section 34 (Specific registration obligation for certain types of entities)

Section 34 transposes Article 27(2) to (5) of the NIS 2 Directive.

Re paragraph 4

Paragraph 4 provides that the Federal Office may, for example, provide for the use of an online form or form for registration in order to facilitate uniform data collection.

Re Section 35 (Information obligations)

Re paragraph 1

Paragraph 1 transposes sentence 2 of Article 23(1) of the NIS 2 Directive.

If the provision of services is affected by particularly important and important entities as a result of significant incidents that have occurred, this may also regularly lead to further restrictions, including indirect restrictions, on the recipients of those services. This may be the case, for example, when these services are used by the recipients to provide additional or other services to third parties. Such supply-chain attacks are regularly difficult to withstand, as the effects of the damage may occur with a delay, in other locations and in companies not directly affected by the original security incident. Examples of such supply-

chain attacks that caused further harm to non-participating third parties include the publicly known incidents on solar winds (2020), Kaseya (2021) or ViaSat (2022). In order to increase the resilience of the economy as a whole in relation to such attacks, it may be necessary, on a case-by-case basis, for the Federal Office to instruct relevant entities affected by a security incident to inform the recipients of their services of the incident so that they can in turn implement the necessary measures to avoid any further damage to their own services. The Federal Office shall inform the competent federal supervisory authority of an order pursuant to this provision.

Re paragraph 2

Paragraph 2 transposes Article 23(2) of the NIS 2 Directive. Service recipients cannot take action against cyber threats themselves in all sectors. It is precisely when supplying electricity or goods that the recipients are not themselves exposed to the cyber threat, but only its consequences. In sectors where the services themselves interact with the information systems of the recipients of the services, it is often useful to inform recipients. The entities must therefore inform them of the threat itself and of possible measures that the beneficiaries themselves may take to protect them.

Re Section 36 (Feedbacks from the Federal Office to reporting entities)

Re paragraph 1

Paragraph 1 transposes Article 23(5) of the NIS 2 Directive. If a criminal background is suspected in the significant incident, the Federal Office shall also provide guidance on how to report the incident to the law enforcement authorities. The Federal Office will provide guidance on how to report the incident to the law enforcement authorities on its website and, where appropriate, refer to it.

Re paragraph 2

Paragraph 2 transposes Article 23(7) of the NIS 2 Directive. Only the Federal Office, as a central body under the NIS 2 Directive, has the information and situational picture to issue corresponding national information.

Re Section 37 (Exemption notice)

Section 37 transposes Article 2(8) of the NIS 2 Directive. This makes use of the possibility of creating an exception. The reason for a partial or complete exemption from the obligations laid down in Articles 21, 23 and 27 of the NIS 2 Directive – transposed in Sections 30 et seq. – is to safeguard the national security interest. Thus, recitals 9 and 10 of the NIS 2 Directive require that, in order to safeguard essential interests of national security, the protection of public order and public security of the Member States, it must be necessary to exempt entities from the above obligations where such information or disclosure would be contrary to the national security interest. As relevant areas, Article 2(8) of the NIS 2 Directive lists the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. In order to meet the notion of a non-excessive exception, a balance must be struck between a ‘high common level of cybersecurity’ (see recitals 138, 142 of the NIS 2 Directive; express objective of the NIS 2 Directive) and the Member State interest of safeguarding national security interests.

This exemption decision must be based on a non-favourable administrative act. In accordance with sentence 2 of section 48(1) of the VwVfG, the legal definition defines the advantage as follows: An administrative act is favourable if it creates or confirms a right or a legally significant advantage. A right could be based on the fact that the entity subject to the exemption, either in whole or in part, complies with the obligations laid down in ParagraphSection 30 et seq. do not have to comply. On the other hand, these obligations are

not simply removed. An advantage must be assessed on the basis of the objective regulatory content of the administrative act in the light of the purpose of the provision on which it is based, namely that an exemption from the above obligations does not benefit the body which receives the exemption decision but the national security interest. The exemption decision is not intended to confer a right, but only to organise the obligations of the addressee of the exemption decision in a different way, especially since equivalent measures equivalent to those of the exemption (see Sections 30 et seq.) must be taken.

For federal administrative bodies, an additional possibility of introducing derogations from the provisions of Part 3 is additional to: Section 46(5) regulated.

Re paragraph 1

Firstly, the above objective is met by a limited right of proposal, by the Federal Chancellery, the Federal Ministry of Defence, the Federal Ministry of the Interior and Community, the Federal Ministry of Justice and the Ministries of the Interior and Justice of the Länder. There is deliberately no provision for the right of the entity concerned to apply. The areas covered by the facilities continue to be restrictive. In particular, reference is made to the legally recognised categories of public security and public order, also explicitly mentioned in the NIS 2 Directive. Recital to be included as a limitation of the exemption should be based on the materiality of the interests of national security.

Last but not least, on the other hand, the high common level of cybersecurity needs to be ensured by implementing equivalent measures (see recitals 13 and 137 of the NIS 2 Directive). Reference is made to recital 137 of the NIS 2 Directive, which provides for a high level of responsibility for cybersecurity risk management measures and reporting obligations. This is to be taken into account by the fact that paragraph 1 provides that, in the case of an exception, the entity shall comply with equivalent requirements. Control of compliance would be the responsibility of the proposing department

Re paragraph 2

Paragraph 2 transposes sentences 1 and 2 of Article 2(8) of the NIS 2 Directive. Paragraph 2, sentence 1, implements the possibility of creating a derogation as provided for in the Directive. Paragraph 2 provides for a simple exemption decision, exemption from risk management measures and reporting obligations. As already noted above, sentence 2 refers to the creation of equivalent standards for the protection of information security.

Re paragraph 3

Paragraph 3 transposes the Article 2(8), sentence 3 of the NIS 2 Directive.

Paragraph (3) introduced the possibility of a full exemption from both risk management measures and reporting obligations as well as registration obligations under a so-called ‘extended exemption notice’. For this purpose, the entities concerned must operate or provide services only in the areas referred to above. Sentence 2 ensures that equivalent measures are maintained.

Re paragraph 4

Paragraph 4 transposes Article 2(9) of the NIS 2 Directive.

Re paragraph 5

Paragraph 5 provides for the revocation of a lawful exemption. In order to revoke a lawful exemption, Paragraph 49 of the VwVfG should be derogated from in order to meet the specific interests of the provision. Paragraph 5, sentence 1 governs the situation in which

the conditions for issuing an exemption decision are subsequently abolished. Sentence 2 provides for a reverse exception if the conditions are only temporarily removed.

Re Section 38 (Obligation to implement, monitor and train business managers of the particularly important entities and important entities)

Section 38 transposes Article 20 of the NIS 2 Directive.

Re paragraph 1

Paragraph 1 transposes Article 20(1) of the NIS 2 Directive and the obligations of corporate management laid down therein. Under that obligation, the management must first approve the specific measures to be taken as suitable and monitor their implementation on an ongoing basis. Even in the case of assistance, the management body remains ultimately responsible. For federal administrative bodies, the responsibility of the management in: Section 43(1) regulated.

Re paragraph 2

Paragraph 2 transposes Article 20(1) at the end of the NIS 2 Directive. The internal liability of the management body in the event of breach of obligations under the BSI Act is in principle based on the general principles (e.g. Section 93 AktG). For legal forms for which no such internal liability exists under the applicable company law provisions, the provision provides for a catch-all provision. In the case of public officials, the existing liability of public officials is therefore not extended in this respect, in the light of the second subparagraph of Article 20(1) of the NIS 2 Directive. For federal administrative bodies, the responsibility of the management in: Section 43(1) regulated.

Re paragraph 3

Paragraph 3 transposes Article 20(2) of the NIS 2 Directive with regard to business management. Important and particularly important institutions are encouraged to provide such training to all employees. For the purposes of this provision, ‘regular’ means training provided at least every 3 years. By way of derogation, Federal administrative bodies apply: Section 43(2).

Re Section 39 (Demonstration obligations for operators of critical installations)

Section 39 continues the previous Section 8a. The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account.

When determining the date for the first submission of evidence under this Law, the Federal Office shall take into account a last submission of evidence under the old legal situation in so far as the evidence is provided continuously approximately every three years.

Re paragraph 1

Paragraph 1 continues the previous Section 8a(3).

Regulation (EC) 300/2008 in conjunction with the Annex to Implementing Regulation (EU) 2015/1998 and Regulation (EU) 2018/1139 lays down extensive safety requirements for operators in the air transport sector. The Federal Office may take such evidence into account in accordance with the above-mentioned Regulations for the fulfilment of the burden of proof under this provision.

Re paragraph 2

Paragraph 2 continues the previous Section 8a(5).

Re paragraph 3

In order to invalidate the Federal Office's verification of the evidence submitted by the operators of critical installations, it is stipulated here that not all the evidence must be submitted to the Federal Office on the same date, but that the Federal Office must give each operator a separate date of proof. The Federal Office must ensure that all operators have at least three years to provide any evidence. For operators of critical installations which were required to provide evidence before the entry into force of this Act as critical infrastructure operator pursuant to Section 8a BSIG in the versions of the First IT Security Act and the IT Security Act 2.0, the starting point here shall be the date of the last proof under the former legal situation.

Re Section 40 (National liaison office and single reporting and contact point for particularly important and important entities)

Section 40 continues the previous Section 8b. The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account.

The amended provision transposes Article 8(3) to (5) of the NIS 2 Directive. In order to increase the resilience of the economy across Europe, the NIS 2 Directive provides, inter alia, for a coordinated exchange of information between Member States and with Union bodies. This is done centrally for Germany via the Federal Office in its capacity as a central body under the NIS 2 Directive.

Re paragraph 1

Paragraph 1 continues the previous Section 8b(1). The amended provision transposes Article 8(3) to (5) of the NIS 2 Directive.

Re paragraph 2

Paragraph 2 transposes Article 8(4) and (5) of the NIS 2 Directive.

Re paragraph 3

Paragraph 3 continues the previous Section 8b(2).

Re subparagraph 1

Point 1 continues the former Section 8b(2)(1).

Re subparagraph 2

Point 2 continues the previous Section 8b(2)(2).

Re subparagraph 3

Point 3 continues the former Section 8b(2)(3).

Re subparagraph 4

Re letter a

Point (a) continues the former Section 8b(2)(4)(a). The rule is adapted to the new categories.

Re letter b

Point (b) continues the former Section 8b(2)(4)(d).

Re letter c

In order to fulfil its tasks, the Foreign Office relies on information on security incidents reported by important and particularly important entities and bodies of the federal administration, which are of foreign policy importance. The Federal Office is obliged to inform the Foreign Office without delay of security incidents with an international dimension.

Re Letter d

Point (d) continues the previous Section 8b(2)(4), points (b) and (c). The scope covers important and particularly important entities. The transmission concepts already agreed between the Federal Government and the Länder in the context of the previous rules can continue to apply to the transmission of registration data and incident reports (‘red-reports’).

Re paragraph 4

Re subparagraph 1

Point 1 transposes Article 8(3)-(5) of the NIS 2 Directive.

Re subparagraph 2

Point 2 transposes Article 23(8) of the NIS 2 Directive.

Re subparagraph 3

Point 3 transposes Article 23(6) of the NIS 2 Directive.

Re paragraph 5

Paragraph 5 continues the previous Section 8b(4a).

Re paragraph 6

Paragraph 6 continues the previous Section 8b(7).

Re Section 41 (Prohibition of the use of critical components)

Re paragraph 1

Paragraph 1 continues the previous Section 9b(1).

Re paragraph 2

Paragraph 2 continues the previous Section 9b(2).

Re paragraph 3

Paragraph 3 continues the previous Section 9b(3).

Re paragraph 4

Paragraph 4 continues the previous Section 9b(4).

Re paragraph 5

Paragraph 5 continues the previous Section 9b(5).

Re paragraph 6

Paragraph 6 continues the previous Section 9b(6).

Re paragraph 7

Paragraph 7 continues the previous Section 9b(7).

Re Section 42 (Request for information)

Section 42 replaces the former Section 8e. The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account.

As a result of its activities as competent authority, CSIRTs and one-stop shops, the Federal Office receives a large number of new information under the NIS 2 Directive on essential and important entities and their IT security threats. These may be sensitive both individually and in total. The Freedom of Information Act provides for a refusal only if the information released is, in itself, sensitive and therefore allows for research by means of requests for access to information which, in themselves, are aimed at insensitive information but which, in sum, make it possible to merge into a sensitive picture of information security of particular importance and importance. In view of the geopolitical situation and the increasing risk of cyber-attacks, including by hostile states, this information must therefore be particularly protected. Article 11(1)(d) NIS 2 Directive therefore also requires the confidentiality of cybersecurity entities to be ensured. This provision is without prejudice to the rights of access to the file of parties to proceedings in the context of opposition and judicial proceedings against orders issued by the Federal Office.

On Chapter 3 (Information security of federal administration facilities)

Re Section 43 (Information security management)

Section 43 creates a new central rule to enshrine essential principles of information security management in the federal administration by law.

Re paragraph 1

Paragraph 1 serves to allocate responsibility in principle for information security and sets out the obligations associated with it and which are further specified in this chapter. Responsibility for ensuring information security lies with the management of an institution as part of the overall management responsibility. It is responsible for compliance with legal and other requirements. These include: Section 44(2) the BSI minimum standards, as well as for federal ministries and the Federal Chancellery pursuant to Section 44(2) the IT baseline protection prescribed by the Federal Office, which is substantively compatible with ISO/IEC 27,001, which belongs to the ISO/IEC 27,000 series referred to in recital 79 of the NIS 2 Directive. This is without prejudice to the existing sub-statutory provisions of

the Cabinet Decision UP Federal Government. It is also responsible for internal arrangements, taking over residual risks and providing information security resources. The Head of Institution is responsible for overarching decisions regarding the information security objectives and the information security strategy. It shall also strike the right balance between IT operations and information security on a case-by-case basis, by actively promoting cooperation between IT operational controllers and information security officers. This includes, among other things, the use of resources to support information security according to needs.

Re paragraph 2

Paragraph 2 transposes Article 20(2) of the NIS 2 Directive. Another element of this paragraph of the NIS 2 Directive provides for continuous awareness-raising among all employees of an institution. This requirement, in particular in relation to phishing and social engineering as referred to in recital 89 of the NIS 2 Directive, is already covered by: Section 44(2) with reference to IT baseline protection. Services provided by the central training service provider of the federal administration, the Federal Academy for Public Administration in the Federal Ministry of the Interior and Community, are guaranteed by the Federal Office for all federal administration institutions. This means that parts of the requirements of the Federal Government's 2017 implementation plan are implemented in a mandatory manner.

Re paragraph 3

Paragraph 3 is a general clause for the purpose of allocating responsibility to installers in the case of entrustment of public service providers – for example at Land level – or private service providers, as already applied under Chapter 7 of the Bund Implementation Plan. It lays down the requirement that bodies organised under public or private law which are entrusted with the provision of services (e.g. service or operational services) for federal information technology must be required to comply with the conditions for ensuring information security. The responsibility is the management of the commissioning body of the Federal Administration (contracting authority). The obligation shall be made to the extent necessary and proportionate to the specific subject matter of the contract or the service entrusted to it. The obligation usually includes the implementation of basic IT protection and relevant minimum standards. Necessary inspection/control rights and cooperation with the contracting authority or the Federal Office to report and resolve incidents or security incidents (e.g. information and cooperation obligations) must also be regulated (linked, where necessary, with appropriate contractual penalties). At the time of commissioning, the Federal Office's powers of inspection and order, which the contracting entity is responsible, must also be extended by contract to the service providers.

Re paragraph 4

Sentence 1 makes it clear that the registration obligation under Section 33 in accordance with Section 29 also applies to entities of the federal administration. The evidence to be provided pursuant to sentence 2 serves, inter alia, to establish transparency on the information security situation in the federal administration. This ensures that an overview of the state of implementation in the federal administration can be established five years after the entry into force of the Act and regularly thereafter. Proof of compliance with the requirements may be provided gradually in accordance with a prioritisation set by the Federal Office on the basis of urgency. The provision transposes Article 32(2)(g) of the NIS 2 Directive and provides that evidence is not only to be provided 'in an appropriate manner', but also that federal administrative bodies must act 'in accordance with the instructions of the Federal Office'. First of all, provision is made for the form of a standardised self-declaration in which the institutions demonstrate the implementation of basic IT protection and minimum standards, unless the Federal Office already has sufficiently up-to-date results of its own audits according to Section 7 available for each institution. Within the federal

administration's institutions, the required detection density can thus be further differentiated on a risk basis and the audit effort in the context of: Section 7 be reduced equally for audited institutions and the Federal Office, where the risk situation allows it.

Re paragraph 5

Sentence 1 continues the previous Section 4(3). Sentence 2 continues the previous Section 4(4). Sentence 3 is added to allow for a significantly better overall assessment of the risk situation with the relevant information ('zero reporting'). In order to avoid inferences, the Federal Intelligence Service and the Federal Office for the Protection of the Constitution are exempted from zero notifications. The concepts of the rules are consolidated by federal authorities into federal administrative entities and from 'IT other authorities' to 'communication technology of the Federal Government', thus placing the protected interest at the centre of the regulation. In view of the protected interest and in the light of the evolving threat landscape, the extension of the scope by extending it to include federal administration institutions is appropriate.

Re paragraph 6

Paragraph 6 continues the previous Section 4(6). The previous reference to the advice of the Federal Government's IT officers is replaced by 'the departments' in order to keep the implementation of the law in place irrespective of different political developments in the organisation of IT governance bodies over the legislative periods. The approval of the portfolios may be given by majority decision in an appropriate body. As in the Bund Implementation Plan, the term 'Ressort' is used in connection with rules concerning the Federal Chancellery or a Federal Ministry, including the business area.

Re Section 44 (References of the Federal Office)

Re paragraph 1

The provision continues the previous Section 8(1). Legal adjustments have been made in order to formulate the provision as a reference rather than an enabling provision. The minimum requirements to be met are governed by the current versions of the minimum standards on the BSI website (current URL: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html) are published and are permanently accessible.

Re paragraph 2

The provision builds on the previous Section 8(1) and enshrines, in addition to the minimum standards already laid down therein, the Federal Chancellery and the Federal Ministries also enshrines IT-Grundschutz, which has already to be implemented by a Cabinet decision on the Federal Government's implementation plan. The IT baseline protection currently consists of BSI standards 200-1, 200-2, 200-3 and the IT baseline protection compendium. The wording open to development in the case without numbering includes its successor standards and the further development of the components of basic IT protection. The minimum requirements to be met are determined by the current versions of the basic IT protection elements on the BSI website (current URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html) are published and are permanently accessible. The concept of 'minimum requirements' was taken over from the Federal Government's implementation plan. In addition to these minimum requirements, each institution may implement further information security measures on a case-by-case basis, depending on the risk assessment. In addition to the minimum standards, basic IT protection is indirectly given the status of law for the Federal Ministries and the Federal Chancellery. For the remaining entities of the federal administration, the implementation of the basic IT protection is unaltered by the existing sub-statutory Cabinet Decision UP Bund. By the deadline of

five years from the date of entry into force (Section 43(4), sentence 2) if financial and human resources remain scarce, it must be ensured that basic IT protection is as efficient and non-bureaucratic as possible. The Federal Office will therefore modernise the IT baseline protection system so as to reduce the scope and the documentation requirements arising from implementation to the minimum necessary, prioritise the requirements and make it possible to use automation tools as far as possible.

Re paragraph 3

Taking into account the recitals of the NIS 2 Directive on risk management requirements, in particular recitals 78 to 82, and the fact that an institution with an ISO 27,001 certificate based on IT baseline protection can demonstrate that the implemented information security measures meet recognised international standards, it is established that the IT baseline protection combined with the minimum standards provided by the Federal Office the risk management requirements under: Section 30 and, consequently, if there are different technical terms, the level of protection laid down in that provision is materially achieved. Where the European Commission adopts implementing acts to this end, priority shall be given to them until they are integrated into basic IT protection or minimum standards. The existing requirements of the Federal Office will then only have a practical effect in so far as the implementing acts leave room for interpretation.

Re paragraph 4

The Federal Office's advice is supplemented by the preparation of tools in accordance with: Section 3(1) No 17 and support for the provision of corresponding solutions by the Federal IT service providers. In the event of additions to the above-mentioned requirements, the Federal Office makes a rough estimate of expenditure as part of the consultation procedure.

Re paragraph 5

The provision continues the previous Section 8(2), supplemented by the provision of reference architectures.

Re paragraph 6

The provision continues parts of the former Section 8(3). This includes the power to specify the use of the federal administration's facilities. The general power of the Federal Office to provide IT security products shall remain with: Section 19 in Part 2. For objective reasons, responsibility for the terms of use is transferred to the Federal Ministry of the Interior and Community in agreement with the other departments (e.g. by a majority decision in an appropriate body) and the terminology is expanded in a uniform manner to 'bodies of the federal administration'. The extension takes place in the light of the fact that an obligation to retrieval via the Federal Office can only be made if there are objective reasons, so that, as a result, the protection of federal information technology security outweighs the autonomy of the federal administration's entities. Procurement law aspects remain unaffected and must be included in the decision-making process. On the basis of the Cabinet decision on IT consolidation, IT security products can also be made available by other federal administration bodies.

Re Section 45 (Information security officers of the federal administration entities)

The new provision introduces information security officers (ISBs) at legal level as a necessary function in federal administration facilities, as already provided for in the Federal Government Implementation Plan. This underlines the paramount importance of information security in all areas of modern administration. A clear legal definition of their tasks and powers also facilitates improved cooperation with the respective management, as well as with other areas of responsibility and their officers, such as data protection and secu-

rity. The federal implementation plan has so far used the name IT security officer (IT-SiBe), which has become obsolete, and this is now being overcome in favour of the ISB.

Re paragraph 1

Paragraph 1 enshrines the importance of the role of information security officers in the institutions of the federal administration and ensures that the function can also be performed in the event that the person primarily responsible for this task is prevented, in order, for example, to avoid delays caused by absentia in connection with digitisation projects.

Re paragraph 2

Paragraph 2 sets out the conditions under which institution ISIs perform their functions. The ISBs shall, inter alia, be enabled by means adapted to their needs, also taking into account the potential for damage caused by security incidents or incidents, as well as the necessary expertise. Although specialist knowledge is not a prerequisite for the transfer of the activity, it must be acquired at least as part of the activity. On the one hand, this will make it easier to fill the corresponding posts in the context of the current shortage of skilled workers. On the other hand, established officials also need to continuously adapt their skills to changing needs. Certification at the Federal Academy for Public Administration (BAköV) to serve as an information security officer can serve as proof of expertise within the federal administration. Technical supervision is carried out in order to ensure the necessary operational independence for the effective representation of security concerns by the competent department ISIs. In the highest federal authorities without business or subordinate authorities, the roles of the institution-ISB and the department-ISB are carried out in staff union.

Re paragraph 3

Paragraph 3 sets out the tasks of the entity ISIs responsible for the operational implementation and control of information security management activities on behalf of their entity management. By complying with the requirements of the Federal Office in accordance with: Section 44(1) comply with the requirements of basic IT protection and minimum standards, they fully comply with the obligation to draw up and implement the information security concept. Additional security measures that ISBs consider necessary on a case-by-case basis may be added to the information security concept, without the omission of such measures constituting a breach of obligations under their individual responsibility. This does not affect the responsibility of the management of the installation. Drawing up the concept is not a very personal task. In particular, the overall information security policy may also provide for outsourcing or entrusting third parties with the development of information security policies. The purpose of the reporting obligation is to achieve compliance, the continuous maintenance of which is conducive to reporting at least quarterly. The frequency specifically appropriate for regularity also depends on the circumstances of each individual case, taking into account the potential for damage. At the same time, the tasks give rise to appropriate powers within the institution, such as the power to review the state of implementation of security policy measures by other organisational units of the institution and the power to request their implementation. In order to avoid conflicts of interests and roles, e.g. between information security and IT management, it is essential that the ISIs are able to carry out their reporting and advisory tasks independently and without notice.

Re paragraph 4

Paragraph 4 grants entities' participation and presentation rights and ensures that they may not be dismissed or discriminated against on account of the performance of their tasks. In order to avoid parallel/double responsibilities, the participation obligation does not apply to measures which are primarily related to information security, for which sepa-

rate regulatory regimes and responsibilities exist (e.g. data protection, security of information, emergency/crisis management, health and safety at work, fire safety). The right to speak to the management of the institution and the relevant department-ISB serves to shape the position of the ISBs as technically independent of the organisation of the institution as is necessary for the task of avoiding conflicts of interest.

Re Section 46 (Departmental Information Security Officer)

The new provision provides a legal basis for ISBs at departmental level (Ressort-ISBs), as they have been designed to date in the context of the Bund implementation plan. In order to implement Article 31(4) of the NIS 2 Directive, it is necessary to ensure operational independence for the oversight of public administration entities. This operational independence is achieved by (a) being able to carry out their reporting and advisory tasks independently and without discrimination, (b) acquire expertise, i.e. not political functions, but focus on technical expertise, (c) have their own budget law in order to be able to act, and (d) independence with regard to information security issues is ensured by allowing portfolios to present themselves directly before the CISO Bund, which in turn has the right to speak directly to legislative bodies. Since there are also supreme federal authorities that do not belong to any department, the role of a department-ISB must also be established for ‘department-independent’ supreme federal authorities. Further provisions in this paragraph, which are laid down for the respective portfolio of the information security officer, shall apply mutatis mutandis to the supreme federal authority and its business area.

Re paragraph 1

Paragraph 1 governs the appointment and responsibility of portfolio ISIs. They are responsible for the functioning and effective management of information security in their portfolio, which includes the relevant supreme federal authority, together with their respective business areas. In the case of supreme federal authorities, the functions must be distinguished from the department and the entity-ISB, but may be delegated to the same person. The adequacy of information security shall be assessed in terms of interactions with IT operational concerns.

Re paragraph 2

Paragraph 2 sets out the conditions under which portfolio IIBs perform their functions. The ISBs’ skills include the use of resources appropriate to their needs and the necessary expertise. Although expertise is not a prerequisite for the transfer of the activity, it must be acquired at least as part of the activity, as the department-ISBs must be able to supervise the ISBs of the entities in their area of competence. On the one hand, this will make it easier to fill the corresponding posts in the context of the current shortage of skilled workers. On the other hand, established officials also need to continuously adapt their skills to changing needs.

Re paragraph 3

Paragraph 3 sets out the tasks of the departmental ITIs, which at the same time confer the power to supervise and implement them internally. As the set-up ISIs are subject to the technical supervision of the department ISIs, the department ISIs are authorised to issue instructions to the business unit in this respect. In order to avoid conflicts of interests and roles, such as between information security and IT management, it is important that the ISIs in charge are able to carry out their reporting and advisory tasks independently and without notice. The reporting obligation serves as a means of promoting compliance.

Re paragraph 4

The veto right to use certain IT products serves the purpose of enforcing information security concerns when needed. The obligation to state reasons prevents this possibility from

circumventing other requirements, e.g. in the context of IT consolidation. The possibility to only partially prohibit use allows a distinction to be made between different applications, for example where products have to be used for the purpose of verification or where it is possible to be used in certain IT environments, but for security reasons it is not intended to be used in general business operations.

Re paragraph 5

Paragraph 5 provides for the possibility for portfolio ISIs to issue exemption decisions for entities within their remit. Entities that meet the requirements of the Section 28(1), sentence 1 or Section 28 (2), sentence 1 cannot be covered; these would be subject to exemption decisions under Section 37. This ensures that federal administration entities that are to be covered by the scope of the implementation of the NIS 2 Directive cannot be exempted from the obligations of the NIS 2 Directive. By way of an exemption decision, a department-ISB may exempt entities in its portfolio from the obligations under Sections 28 to 50, as long as there are objective reasons for granting the exemption and there are no identifiable adverse effects on the Federal Government's information security. For example, there may be objective reasons if an indirect federal administration body has a very small number of employees and locations and/or has outsourced its IT operations. Apparent adverse effects on the Federal Government's information security may arise, in particular, if the entity poses a potential risk of interconnection for other federal entities; for example, if the entity is connected to the federal networks or uses services of the Federal Government's IT consolidation.

Re paragraph 6

Paragraph 6 grants portfolio ISIs rights of participation and presentation and ensures that they may not be dismissed or penalised for the performance of their tasks. In order to avoid parallel/double responsibilities, the participation obligation does not apply to projects which are primarily related to information security, for which separate regulatory regimes and responsibilities exist (e.g. data protection, security of information, emergency/crisis management, health and safety at work, fire safety).

Re Section 47 (Major digitalisation projects and communication infrastructures of the Federation)

Re paragraph 1

Paragraph 1 provides for the appointment of its own ISBs for essential digitisation projects and communication infrastructures of the Federal Government. Due to the increasing importance, size and complexity of IT projects and structures, federal administrative bodies may classify them as significant digitisation projects under paragraph 2, which implies the technical need to appoint their own ISBs for the project.

Re paragraph 2

In the case of cross-departmental digitisation projects, such as the IT consolidation of the Federal Government, it is to be assumed that it is essential for general security concerns, and cross-government communication infrastructures, such as the federal networks, are of paramount importance for government communication as a whole.

Re paragraph 3

Paragraph 3 lays down the responsibility for appointing the ISB. The decision-making competence of the Federal Ministry of the Interior and Community in cases of doubt, where an agreement on the responsibility to appoint an ISB cannot be reached in an appropriate body, serves to resolve possible conflicts and to ensure that the performance of the function is not delayed or hindered by questions of competence.

Re paragraph 4

It is up to the relevant department to decide whether the ISB is under the management of the entity or the relevant ISI.

Re paragraph 5

Paragraph 5 continues the previous Section 8(4). In order to ensure information security in the planning and implementation of major digitisation projects, the use of means for information security that meet the needs of the relevant information security officer and the expertise of the relevant information security officer.

Re Section 48 (Office of the Information Security Coordinator)

The new provision governs the appointment of a coordinator of the Federal Government for Information Security (CISO Bund). Specific organisational links and involvement in relevant bodies are reserved for the implementing Cabinet decision. In order to avoid conflicts of interest, the function should be organised as independently as possible.

On Part 4 (Databases of domain name registration data)

Part 4 transposes Article 28 of the NIS 2 Directive.

Re Section 49 (Obligation to maintain a database)

Re paragraph 1

Paragraph 1 transposes Article 28(1) of the NIS 2 Directive.

Paragraph (2)

Point 1

Point 1 transposes Article 28(2)(a) of the NIS 2 Directive.

Re subparagraph 2

Point 2 transposes Article 28(2)(b) of the NIS 2 Directive.

Re subparagraph 3

Point 3 transposes Article 28(2)(c) of the NIS 2 Directive.

Re subparagraph 4

Point 4 transposes Article 28(2)(d) of the NIS 2 Directive.

Re paragraph 3

Paragraph 3 transposes Article 28(3) of the NIS 2 Directive.

Re paragraph 4

Paragraph 4 transposes Article 28(4) of the NIS 2 Directive.

Re paragraph 5

Paragraph 5 grants the Federal Office competence to carry out an examination.

Re Section 50 (Obligation to grant access)

Section 50 implements Article 28(5) of the NIS 2 Directive. A request from a legitimate access seeker shall be considered justified if the applicant demonstrates a legitimate interest. This is regularly the case where the application is accompanied by a reference to an administrative operation and the requested information is appropriate, necessary and proportionate to the performance of the applicant's tasks. When checking the requirements, the Federal Office may, with regard to the procedure for granting access and the proper keeping of the database, require the obliged entities to provide the records, documents and other documents necessary for that purpose in the Federal Office's view in an appropriate manner and provide information.

Re Section 51 (Obligation to cooperate)

Section 51 implements Article 28(6) of the NIS 2 Directive. The obligation to cooperate is not exclusively aimed at avoiding double collection of domain name registration data. In principle, it refers to all of the following: Section 49 and Section 50 established obligations, including e.g. the request response and the process of issuing registration data. Rationale and purpose of double addressing Top Level Domain Name Registries and Domain Name Registration Service Providers in Section 49 and Section 50 it is not that they fulfil all the obligations twice, but must cooperate in the framework of an agreed division of labour, as is already the case to a large extent. Registration data shall not be collected, verified and stored twice. The obligation to cooperate ensures the fulfilment of the obligations without duplication of databases. An obligation to run double databases would lead to a significant outflow of registration data to non-EU countries, as a large number of registries and registrars are based there.

On Part 5 (Certification, declaration of conformity and marking)

Re Section 52 (Certification)

Re paragraph 1

Paragraph 1 continues the previous Section 9(1).

Re paragraph 2

Paragraph 2 continues the previous Section 9(2).

Re paragraph 3

Paragraph 3 continues the previous Section 9(3). The Federal Academy for Public Administration continues to offer training and certification to the information security officers of the federal administration, as set out in the 2017 Federal Implementation Plan.

Re paragraph 4

Re subparagraph 1

Point 1 continues the former Section 9(4)(1).

Re subparagraph 2

Point 2 continues the former Section 9(4)(2).

Re paragraph 5

Paragraph 5 continues the previous Section 9(4a).

Re paragraph 6

Paragraph 6 continues the previous Section 9(5).

Re paragraph 7

Re subparagraph 1

Point 1 continues the former Section 9(6)(1).

Re subparagraph 2

Point 2 continues the former Section 9(6)(2).

Re paragraph 8

Paragraph 8 continues the previous Section 9(7).

Re Section 53 (Conformity assessment and declaration of conformity)

The provision aligns IT security conformity assessment procedures with international standards and in particular the Cybersecurity Act (CSA) Regulation (EU) 2019/881, which also applies in the NIS2 Directive. The CSA also provides, as part of a certification scheme, for a self-assessment of conformity as an alternative to classic third-party certification, where a manufacturer or provider of ICT products, ICT services or ICT processes itself carries out all verifications to ensure that the ICT products, ICT services or ICT processes comply with the European cybersecurity certification scheme. The self-assessment involves the signature of a declaration by the manufacturer, provider or IT security service provider confirming compliance with the requirements of the Technical Directive (declaration of conformity). By doing so, the signatory (issuer) assumes responsibility for compliance. The benefits of self-assessment are the lower costs and burden for the manufacturer, provider or IT security service provider. It also allows the Federal Office to establish requirements on IT security at a low level on the market and at the same time to ensure that the requirements are controlled at a level commensurate with the level of protection, without burdening the market with the stricter requirements of certification. The declaration of conformity is a purely national provision. In accordance with Regulation (EU) 2019/881, the Federal Office will not operate a scheme contrary to a European harmonised certification scheme. At the same time, however, the Federal Office can pursue the objective of establishing a well-established national scheme for European harmonisation by means of Regulation (EU) 2019/881.

Re paragraphs 1 and 2

Paragraph 1 lays down the framework for a declaration of conformity. As far as the IT security label is concerned, no consumer products are covered by the declaration of conformity under this Regulation. One possible scope is in particular the IT baseline protection already established in the Federal Office and corresponding self-assessments of individuals (e.g. IT-Grundschutz practitioners) or institutions.

Paragraphs 1 and 2 also clarify that the relevant technical guidelines are drawn up by the Federal Office and specify which specific requirements (in particular with regard to carrying out and demonstrating conformity assessment) are associated with the self-assessment. Both the requirements and the requirements for carrying out conformity assessment may thus vary from the Technical Directive to the Technical Directive. The requirements for conformity assessment can involve established actors (e.g. in the field of basic protection) who already offer a conformity assessment. As clarified in paragraph 3, accredited conformity assessment bodies may also be used.

This approach largely reflects the regulatory content of schemes within the scope of Regulation (EU) 2019/881. The flexibility thus achieved enables the Federal Office to react in the Technical Guidelines to the objectives and specific subject of the self-assessment. On the basis of the good experience with the IT security label, the Federal Office should also be able to provide in the Technical Guidelines for the provision of up-to-date information on the website of the Federal Office and, where appropriate, to link this to the identifier of the scheme by means of a dynamic component.

Re paragraph 3

In addition, in order to ensure a uniform level of conformity assessment, the Federal Office can make use of the system of accreditation in its Technical Guidelines in accordance with the Act on Accreditation Bodies (Akkreditierungsstellegesetz – AkksstelleG). Issuers of a declaration of conformity must then undergo a conformity assessment by a conformity assessment body accredited by the German Accreditation Body (DAkkS), which has been granted the power by the Federal Office, as such within the scope of the Section 53 to take action. The granting of the power is at the discretion of the Federal Office and may be subject to requirements that go beyond those of accreditation. The decision may be accompanied by ancillary provisions. The status of the authority responsible for granting the power is accompanied by the rights of the Federal Office in accordance with the AkkstelleG.

Re paragraph 4

The sentence 1 of paragraph 3 ensures that the Federal Office has, if necessary, the information and documents necessary for supervision. The declaration of conformity to be submitted in accordance with sentence 2 may, in so far as the scheme so provides, be published by the Federal Office on the website of the Federal Office in accordance with paragraph 2, subparagraph 6, together with other information and documents.

Re paragraphs 5 and 6

Unlike certification, the declaration of conformity is not based on a decision of the Federal Office in the form of an administrative act. Therefore, enforcement of supervisory measures requires an autonomous legal basis. Compliance with the requirements is checked ex post by the already established market surveillance of the Federal Office. This can be done without need or on an ad hoc basis. If measures are taken on the basis of a reasonable suspicion, the Federal Office may charge fees to the addressee of the measure. A reasonable suspicion may be based both on the Federal Office's own findings and on trusted public sources or flaggers. Supervision is accompanied by the provisions on penalties in: Section 65. According to that provision, the use of a declaration of conformity declared invalid by the Federal Office or if it is only falsely claimed that such a declaration has been made is punishable by criminal penalties.

Re Section 54 (National cybersecurity certification authority)

Re paragraph 1

Paragraph 1 continues the previous Section 9a(1).

Re paragraph 2

Paragraph 2 continues the previous Section 9a(2).

Re paragraph 3

Paragraph 3 continues the previous Section 9a(3).

Re paragraph 4

Paragraph 4 continues the previous Section 9a(4).

Re paragraph 5

Paragraph 5 continues the previous Section 9a(5).

Re paragraph 6

Re subparagraph 1

Point 1 continues the former Section 9a(6)(1).

Re subparagraph 2

Point 2 continues the former Section 9a(6)(2).

Re paragraph 7

Re subparagraph 1

Point 1 continues the former Section 9a(7)(1).

Re subparagraph 2

Point 2 continues the former Section 9a(7)(2).

Re Section 55 (Voluntary IT security label)

Re paragraph 1

Paragraph 1 continues the previous Section 9c(1).

Paragraph (2)

Point 1

Point 1 continues the former Section 9c(2)(1).

Re subparagraph 2

Point 2 continues the previous Section 9c(2)(2).

Re paragraph 3

Paragraph 3 continues the previous Section 9c(3).

Re paragraph 4

Paragraph 4 continues the previous Section 9c(4).

Re paragraph 5

Re subparagraph 1

Point 1 continues the former Section 9c(5)(1).

Re subparagraph 2

Point 2 continues the former Section 9c(5)(2).

Re subparagraph 3

Point 3 continues the former Section 9c(5)(3).

Re paragraph 6

Paragraph 6 continues the previous Section 9c(6).

Re paragraph 7

Paragraph 7 continues the previous Section 9c(7). The previous reference to paragraph 3 was misleading or incorrect. For this reason, the provision was explicitly issued for the duration. The duration for which the manufacturer or service provider guarantees compliance with the IT security requirements is, as in the past, laid down in the following: Section 56(2) and the procedures set out therein.

Re paragraph 8

Re subparagraph 1

Point 1 continues the former Section 9c(8)(1).

Re subparagraph 2

Point 2 continues the former Section 9c(8)(2).

Re paragraph 9

Paragraph 9 continues the previous Section 9c(9).

On Part 6 (Regulatory appropriations, restrictions on fundamental rights and reporting obligations)

Re Section 56 (Authorisation to issue statutory ordinances)

Part of the provision continues the previous Section 10 of the BSI Act. Because of the requirement in the first sentence of Section 62(2) in conjunction with Section 47(1) of the Joint Rules of Procedure of the Federal Ministries (GGO) to participate in the adoption of statutory ordinances, including specialist circles and associations, the statutory investment order is therefore superfluous in the previous powers to issue statutory ordinances in Section 10 of the BSI Act.

Re paragraph 1

Paragraph 1 continues the previous Section 10(2). The statutory ordinance adopted on the basis of this paragraph may, in particular for the certification of products or components, information technology systems, protection profiles and persons and recognition of expert bodies, lay down the modalities of the certification procedure, such as the submission of applications and possible cooperation obligations, and possible ancillary provisions (such as time limits) of certificates and recognitions.

Re paragraph 2

Paragraph 2 continues the previous Section 10(3). According to the explanatory memorandum to the IT Security Act 2.0, the Regulation may, for example, lay down the details of the design (graphical presentation, etc.). The procedures for determining the suitability of industry-conformed IT security requirements and for applications for clearance by a manufacturer may also be further specified therein. In particular, the precise procedure and design of the reference to security information (e.g. on available security updates or known vulnerabilities), which is to be part of the IT security label, must be regulated there.

Re paragraph 3

Paragraph 3 transposes Article 24 of the NIS 2 Directive. Where information technology products, services or processes are relevant for the provision of services of the entity, mandatory certification of those products, services or processes may contribute to reducing the risk of incidents in those areas. Therefore, in so far as the nature and extent of the entity's risk exposure justifies this intervention, it is foreseen that the BMI may, in implementation of Article 24(4) of the NIS 2 Directive, require certification in these areas. This provision applies only to the extent that corresponding certification schemes are also in place. Before the adoption of the statutory ordinance, the BMI and with the involvement of the potentially affected entities must verify that sufficient availability on the market is ensured for the products, services or processes to be included.

Re paragraph 4

Paragraph 4 continues the previous Section 10(1). The results of the evaluation of this standard in accordance with Article 6(1)(1) of the Second Act on Increasing the Security of Information Technology Systems have been taken into account. The current practice of consulting representatives of the scientific community, the operators concerned and business associations is maintained (cf. Section 62(2) in conjunction with Section 47(3) GGO).

This draft law provides that, in addition to the categories of entities within the category of particularly important entities, which are mandatory under the NIS 2 Directive, KRITIS operators will continue to be defined on the basis of supply-related thresholds. This is necessary in order to achieve consistency with the KRITIS Common Law and the KRITIS provision procedure provided for in the CER Directive. At the same time, the evaluation of KRITIS related elements of the IT Security Act 2.0 showed that, due to the sharp extension of the scope of the BSI Act in the context of NIS 2 implementation, critical infrastructure should continue to be identified with a focus on supply relevance. Under this Regulation, certain undertakings as KRITIS operators are at the same time considered to be particularly important entities.

In the future, Kritis operators will continue to be determined with thresholds based on their relevance.

For the level of coverage to be defined as significant in the statutory ordinance on the basis of sector-specific thresholds, the procedure of the Regulation on the identification of critical infrastructure (BSI-KritisV), which has already been established in multi-annual administrative practice, is to be continued. In this context, BMI, together with the relevant departments and with the participation of the KRITIS operators and their trade associations, shall determine appropriate scales for critical installations, from which the level of supply can be approximated in the sense of the persons served by the installation. These parameters typically represent quantitative or qualitative plant-specific characteristics, such as capacity, size, type or type of installation, which are either already known to the operators or can at least be determined with the least effort possible for the installations concerned. Thresholds are then laid down for the scales thus found, above which the level of supply of the installation concerned is deemed to be significant within the meaning of this Act and therefore the installation constitutes a critical installation.

Re paragraph 5

Paragraph 5 transposes Article 23(11)(2) of the NIS 2 Directive. The Federal Office can provide guidance on when security incidents are considered significant. Where the European Commission adopts implementing acts to that effect, they shall prevail. The Federal Office's requirements will then only have a practical effect in so far as the implementing acts leave room for interpretation. Feedback from the industry during the drafting of the speaker's draft also suggests that it would be useful to further specify the significance criterion in the context of a statutory ordinance. However, as an implementing act of the European Commission is also planned for this purpose by October 2024, further details at legislative level should be avoided. Otherwise, this would lead to ambiguities or misunderstandings for those applying the law if the provisions of the BSI Act were in force, but if necessary were invalid on the basis of other provisions in the implementing act. This problem does not arise as a result of the possibility of providing further clarifications in addition to the implementing act by means of a downstream regulation.

Re paragraph 6

Paragraph 6 provides for the possibility of shortening the Section 61(3), sentence 5 prescribed time limit by means of a statutory ordinance. If, for example, the health sector becomes the target of cyber-criminals or if new vulnerabilities make successful attacks more likely, it will be possible to respond to the changing cyber threat landscape.

Re Section 57 (Restriction of fundamental rights)

The provision continues the previous Section 11.

Re Section 58 (Reporting obligations of the Federal Office)

The heading makes it clear that reporting obligations always relate to the Federal Office. By contrast, reporting obligations always relate to entities.

Re paragraph 1

Paragraph 1 continues the previous Section 13(1).

Re paragraph 2

Paragraph 2 continues the previous Section 13(2).

Re paragraph 3

Paragraph 3 continues the previous Section 13(3).

Re paragraph 4

Paragraph 7 transposes Article 23(9) of the NIS 2 Directive. The information to be transmitted shall be subject to the exceptions of Articles 2(11) (national, public security or defence) and 13 (confidentiality of trade secrets) of the NIS 2 Directive. The concept of anonymisation shall be interpreted in the sense of pseudonymisation as defined in Article 4(5) of Regulation (EU) 2016/679. The data for the calendar year 2024, which have not yet been submitted on the basis of the previous Section 11(6), are to be transmitted as part of the first transmission during the three-month period prescribed by the NIS 2 Directive.

Re paragraph 5

Re subparagraph 1

Point 1 transposes Article 3(5)(a) NIS 2 Directive.

Re subparagraph 2

Point 2 transposes Article 3(5)(b) NIS 2 Directive.

On Part 7 (Supervision)

Re Section 59 (Responsibility of the Federal Office)

The provision transposes Articles 8(1) to (2), 26(1) NIS 2 Directive. Responsibility for important and particularly important entities is determined by the principle of establishment. Responsibility for operators of critical installations shall be determined on the basis of the geographical location of the critical installations concerned.

Re Section 60 (Central competence in the European Union for certain types of entities)

Re paragraph 1

Paragraph 1 transposes Article 26(1)(b) of the NIS 2 Directive.

Re paragraph 2

Paragraph 2 transposes Article 26(2) of the NIS 2 Directive.

Re paragraph 3

Paragraph 3 implements Article 26(3) of the NIS 2 Directive. A representative may be a natural or legal person established in the European Union, expressly designated to act on behalf of an entity not established in the European Union, to whom the Federal Office may address questions relating to the obligations of the designating entity under this Act.

Re paragraph 4

Paragraph 4 transposes Article 26(4) of the NIS 2 Directive.

Re paragraph 5

Paragraph 5 transposes Article 26(5) of the NIS 2 Directive.

Re Section 61 (Supervisory and enforcement measures for particularly important entities)

Re paragraph 1

The provision transposes Article 32 and Article 31(1) in conjunction with Article 20(2) of the NIS 2 Directive. Since a regular obligation to provide evidence for the implementation of risk management measures applies only to operators of critical installations, it is provided that the Federal Office may exercise the supervisory measures provided for here in respect of individual entities. Under this provision, the Federal Office is empowered, inter alia, to require institutions to have audits, audits or certifications carried out by independent bodies. Even without mandatory audits, audits or certifications, the Federal Office may require individual institutions to provide evidence of compliance with some or all of

the requirements under Sections 30, 31 and 32. If no audits, audits or certifications have been carried out by the body, the Federal Office may require other supporting documents. These include, for example, company-owned policies and documentation, reports or self-declarations. The Federal Office may also check compliance with the training obligation (Section 38(3)).

In accordance with the requirements of the NIS 2 Directive, in the exercise of these supervisory measures in relation to particularly important entities, it is not necessary for the Federal Office to have information or information that justifies the assumption that an entity has failed to transpose or has incorrectly transposed the requirements of Sections 30, 31 and 32. Instead, the Federal Office shall take into account the criteria set out in paragraph 4 when selecting establishments in order to prioritise them. The Federal Office's discretion in selecting facilities is to be interpreted broadly within the meaning of the NIS 2 Directive. The criteria referred to in paragraph 4 shall be used to prioritise the entities to which the supervisory measures should be applied as a matter of priority. On the other hand, the criteria referred to in paragraph 4 are not suitable for exclusion, for example to justify that certain supervisory measures should not apply to individual entities because, for example, they are particularly small or the likelihood of incidents is considered low. In accordance with the requirements of the NIS 2 Directive, the Federal Office must have the power to exercise the supervisory measures referred to here in respect of all particularly important entities.

The competence of the Federal Office for Organisations of Federal Administration shall be based on the powers of the Federal Office in Part Two, Chapter 1 and Part 3.

Re paragraph 6

Paragraph 6 transposes Article 32(4)(b) of the NIS 2 Directive.

Re paragraph 7

Paragraph 7 transposes Article 32(4)(c), (d) and (f) of the NIS 2 Directive. The evidence may be provided through documented IT security policies, process descriptions, policies, data, documents and other information necessary to assess the cybersecurity risk management measures taken by the entity concerned.

Re paragraph 8

The first sentence of paragraph 8 transposes Article 32(4)(e) of the NIS 2 Directive. The second sentence of paragraph 8 transposes Article 32(4)(h) of the NIS 2 Directive.

Re paragraph 9

Paragraph 9 transposes Article 32(5)(1) of the NIS 2 Directive. The national implementation of enforcement measures (suspension, second sentence, point 1) and prohibition (second sentence, point 2) is subject to additional conditions due to the respective severity of the interferences with fundamental rights, in line with the second subparagraph of Article 32(5) of the NIS 2 Directive. For reasons of proportionality, the application of these two enforcement measures is in principle only a measure of last resort. Consequently, less restrictive and equally effective means of enforcing an order issued by the Federal Office must be exhausted beforehand without success, in particular those relating to administrative enforcement under the VwVG. If the Federal Office or the competent supervisory authority is aware of the unreliability of the management from previous administrative procedures, the unsuccessful exhaustion of other means may not be necessary before a prohibition (second sentence, point 2). This is likely to be the case, in particular, if, in previous administrative procedures, only the prohibition (second sentence, point 2) was successful.

The condition ‘where there is a connection between enforcement action and the order’ is intended to ensure that, for example, no authorisation is suspended which is not related to the Federal Office’s information security order to be enforced. For example, no authorisation to store hazardous substances – only physical – is suspended because the entity stores the data of its customers in an activity within the scope of Section 28(1) or (2) without IT safeguards.

Re paragraph 10

Paragraph 10 transposes Article 32(9) of the NIS 2 Directive.

Re paragraph 11

Paragraph 11 transposes Article 35 of the NIS 2 Directive and takes account of the fact that, in the event of infringements of the obligations addressed therein, there may also be infringements of other provisions of EU law. Even if the Federal Office carries out technical checks, not data protection law, within the scope of its competences, it is intended to ensure that, because of the close connection between data security and data protection, in the event of apparent breaches of data protection rules found at random during the audit, the competent authorities are immediately informed and can carry out an audit. The NIS 2 Directive refers to the scope of infringements that may result in a personal data breach, both in the case of insufficient cybersecurity risk management measures and in the event of a failure to comply with the reporting obligations laid down by law. The notification shall be made without undue delay after the technical control of the competent data protection supervisory authority pursuant to Article 55 or 56 of Regulation (EU) 2016/679.

Re paragraph 12

Paragraph 12, transposing Article 37 of the NIS 2 Directive, sets out details of mutual assistance for competent supervisory authorities in other Member States of the European Union when entities provide services in more than one Member State, for example by using IT systems, components or processes located in Germany.

Re Section 62 (Supervision and enforcement measures for important entities)

The provision transposes Article 33 of the NIS 2 Directive. In principle, this provision provides for the same supervisory measures by the Federal Office as in: Section 61 for institutions of particular importance. However, for important entities to exercise those supervisory measures, facts justify the assumption that an important entity has failed to implement the legal obligations or has not correctly implemented the legal obligations.

Re Section 63 (Administrative obligation)

The provision transposes Article 34(6) of the NIS 2 Directive.

Re Section 64 (Infringements committed by social security institutions)

The provision continues the previous Section 14a.

On Part 8 (Fine provisions)

Re Section 65 (additional fines)

The provision continues the previous Section 14. In particular, the fines were supplemented in line with the requirements of the NIS 2 Directive and the framework for fines was adapted.

Re paragraph 1

Paragraph 1 continues the previous Section 14(1). As in the past, paragraph 1 penalises cases in which the evidence, requests for information and indicators to be provided by critical installations operators is deliberately incorrect or incomplete.

Re paragraph 2

Points 1(a), (b), (c) and (d) of paragraph 2 cover cases of infringements of enforceable orders. The purpose of a separate list is to make it possible to impose a fine of varying amounts on account of the different gravity of the infringements.

Re subparagraph 1

Re letter a

The above-mentioned Section 11(6) manages the former Section 5b(6) and the first sentence of Section 16(1), the former Section 7c(1), first sentence, Section 17 the previous Section 7d and the fifth sentence of Section 39(1) continue with the fifth sentence of Section 8a(3).

Re letter b

This penalty continues to be the previous offence under the first sentence of Paragraph 7a(2).

Re letter c

The first sentence of Section 8c(4) is deleted as the category ‘digital service providers’ is included in the new categories of entities.

Variant 1 introduced a new fine to penalise the refusal to provide necessary information to deal with a disruption to operators of critical installations.

It also adds new administrative fines in line with the requirements of Article 32(4)(i) of the NIS 2 Directive for particularly important entities and Article 33(4)(h) of the NIS 2 Directive for important entities:

A fine has been added in accordance with the provisions of the NIS 2 Directive pursuant to Article 32(4)(d) for particularly important entities and Article 33(4)(d) for important entities – transposed into Section 62(3), first sentence, in conjunction with Section 63: This applies to breaches of instructions within a given timeframe to ensure that cybersecurity risk management measures comply with Article 21 or comply with the reporting obligations set out in Article 23.

Section 61 The first or third sentences of paragraph 6, also in conjunction with Section 62, provide for a fine for infringements of particularly important and important institutions against orders pursuant to Section 62(6). This provides that the Federal Office may issue instructions to particularly important and important entities concerning measures necessary to prevent or remedy a security incident or defect. The Federal Office may also require reporting on the measures ordered pursuant to the first sentence. Requirements set out in Articles 32(4)(i) and 33(4)(h) of the NIS 2 Directive are hereby transposed. It follows that an infringement fine must be imposed under Article 32(4)(b) and Article 33(4)(b) respectively.

An infringement of a binding instruction pursuant to the first or third sentences of Section 61(7), in conjunction with Section 62, shall be punished. The creation of this fine transposes Article 32(4)(i) in conjunction with points (c) and (f), and Article 33(4)(h) in con-

junction with points (c) and (f) of the NIS 2 Directive, which provide for a proportionate fine for important and particularly important entities.

Section 62 Paragraph 8, or also in conjunction with Section 62, provides, with respect to particularly important and important entities, that the Federal Office may instruct them to inform the natural or legal persons to whom they provide services or perform activities and who are potentially affected by a significant cyber threat, of the nature of the threat and possible defensive or remedial measures that may be taken by those natural or legal persons in response to that threat. It may also instruct important and particularly important entities to make publicly available information on breaches of this Directive in accordance with certain requirements. The creation of this penalty complies with the requirements of Article 32(4)(i) in conjunction with points (e) and (g) of the NIS 2 Directive and Article 33(4)(h) in conjunction with points (e) and (g).

Re Letter d

A new penalty is added to point (d) in accordance with the requirements of the NIS 2 Directive.

Section 35 The first sentence of paragraph 1 provides that, in the event of a significant incident, the Federal Office may instruct particularly important entities and important entities to inform the recipients of its services without delay of that significant incident, which could affect the provision of the service concerned. Article 34(4) of the NIS 2 Directive provides for a penalty of Article 23(1) of the NIS 2 Directive.

Article 34(7) of the NIS 2 Directive provides for a fine for infringements of the first sentence of Section 36(2).

Re subparagraph 2

In point 2, the references have been adapted. The previous offence created a possibility of imposing a penalty for the non-compliance with the first sentence of Section 8a(1) in conjunction with a statutory ordinance pursuant to the first sentence of Section 10(1) of the Act not, or not correctly, in full or in time. It provided for appropriate organisational and technical arrangements to avoid disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are relevant for the functioning of the critical infrastructure they operate.

The reference has been adapted and now refers to infringements of the newly created Section 30 (risk management measures), which replaces the first sentence of Section 8a(1). It also complies with the requirements of the NIS 2 Directive (Article 34(4) in conjunction with Article 21 NIS 2 Directive) following a fine for breaches of risk management measures.

Re subparagraph 3

A new penalty has been created in point 3, which penalises infringements of the third sentence of Section 30(1) (compliance with the obligation to keep documentation). This takes into account the requirements of the NIS 2 Directive, Article 34(4) in conjunction with Article 21 NIS 2 Directive, here paragraph 4.

Re subparagraph 4

Section 32 The first sentence of paragraph 1 defines the reporting obligations for particularly important and important entities (transposition of Article 23 NIS 2 Directive). This transposes the requirement of a fine under Article 34(4) in conjunction with Article 23(4) NIS 2 Directive.

Sections 8c and 8f shall be deleted as the regulatory addressees are included in the new categories of establishments

Re subparagraph 5

Point 5 provides for a fine if, contrary to the second sentence of Section 32(2), a final declaration is not made or is not made correctly, completely or in good time. Article 34(4) in conjunction with Article 23(4)(e) NIS 2 Directive is hereby transposed.

Re subparagraph 6

According to point 6, any person who fails to provide an information or an amendment, or does not transmit it correctly, completely or in good time, is unlawful. The first sentence of Section 8b(3) shall be replaced by: Section 33(1) and (2) replaced and adapted to the newly created categories of institutions: Paragraph (1) defines the registration obligations for important and particularly important entities, paragraph (2) the requirements for operators of critical facilities.

The first sentence of Section 8f(5) is deleted as it is included in the new categories of establishments. However, this is replaced by Section 34(1) and (2), which provides for registration obligations for other types of entities.

Re subparagraph 7

Point 7 provides for a fine for operators of critical installations. Under the second sentence of Section 33(2), they must ensure that they can be contacted at any time via their contact details referred to in paragraph 1.

Re subparagraph 8

In point 8, a new fine was created. Section 34 Paragraph 2 provides for amendments to be made to Section 34(1) the information to be provided must be sent to the Federal Office without delay and no later than two weeks from the date of the amendment.

Sanctioning is necessary to allow better enforceability of the registration obligations. The purpose of this is to ensure the prompt transmission of important safety information to affected operators. This makes it possible to ensure a reliable, consistent and rapid flow of information in the event of faults and in case of other IT security information that is crucial to the availability and functionality of the operators. Only by extending the obligation to notify changes in a timely manner can they be effectively guaranteed.

Re subparagraph 9

A fine for infringements of the first sentence of Section 35(2), also in conjunction with the second sentence, provides for Article 34(4) in conjunction with Article 23(2) NIS-2 Directive.

Re subparagraph 10

The reference to update the burden of proof (see paragraph 1) has been adapted here: Defined here Section 39(1), first sentence those for critical entities.

Re subparagraph 11

No 11 is sanctioned, unless the requirements or procedures referred to in the first sentence of Section 49(3) are maintained. Points 11, 12 and 13 implement the possibility provided for in Article 36 of the NIS2 Directive to sanction non-compliance with the requirements for measures also for Top Level Domain Name Registries and Domain Name Reg-

istration Service Providers. This creates a enforceability of the legal obligation to maintain a database on the domain(s) and their domain name registration data and to make these data accessible to requesters upon justified request.

Re subparagraph 12

Point 12 provides for a penalty if, contrary to the second sentence of Section 49(3) or (4), the requirements, procedures or data referred to therein are not made available, or are not made available in the prescribed manner or in good time.

Re subparagraph 13

Point 13 shall impose a fine if, contrary to the first sentence of Section 50(1), access is not granted or is not granted in good time.

Re subparagraph 14

Point 14 created a new fine: Section 52 The fourth sentence of paragraph 2 provides that a certificate referred to in the first sentence may be used for a product, service, person or IT security service provider only if the Federal Office has issued such a certificate and it has not been revoked or otherwise invalidated. Penalties in the context of a fine for use contrary to the conditions set out above are necessary because of the potential for abuse and associated unauthorised use; here too, there is no effective possibility of administrative compulsion. A penalty shall also be provided for cases in which, contrary to the fourth sentence of Section 53(1), a declaration pursuant to the second sentence of Section 53(1) is used.

The second sentence of Section 54(6) is a new offence for a fine which penalises the use of revoked cybersecurity certificates or invalidated EU declarations of conformity. A need for penalties arises from comparable potential abuse, the consequences of unauthorised use and the lack of effective administrative compulsion.

Section 55 The first sentence of paragraph 4 continues the previous Section 9c(4), first sentence.

Re subparagraph 15

Section 53 introduced the possibility of making a declaration of conformity itself in accordance with the instructions of the Federal Office and under its supervision. Although the issuer himself bears the responsibility for his declaration of conformity, there is market confidence in the Federal Office’s ability under Section 53 to take action against detected deviations from the underlying requirements. However, this trust presupposes that the Federal Office can also take action against those actors who do not have a valid declaration of conformity within the meaning of Section 53 and who merely deliberately or negligently (for example by using a corresponding mark) claim to have submitted themselves to the requirements of Section 53. Section 53 The second sentence of paragraph 3 provides for a fine when acting as a conformity assessment body without the granting of powers

Section 54 Paragraph 2, sentence 2, continues the previous Section 9a(2), sentence 2. An addition has been made: In accordance with Section 53(3), sentence 2, where accreditation by the Federal Office has been provided for in the Technical Guidelines, powers must be granted for conformity assessment. Where a body carries out conformity assessment activities without having such authority, this jeopardises the comparability of conformity assessment procedures and, consequently, the specific confidence in the declaration of conformity that the requirement should provide.

Re subparagraph 16

The former Section 14(2)(8) with a penalty for infringements of Section 8c(1), sentence 1 has been deleted as it is included in the new categories of establishments.

The provision provides for a penalty for particularly important entities (Section 61(5), sentence 3). Unless entry into a space referred to therein is permitted, fails to produce, or does not produce a document referred to therein, does not provide information, does not provide information, does not provide correct, complete or timely assistance or does not provide assistance in good time.

Re paragraph 3

Paragraph 3 continues the previous Section 14(3).

Re paragraph 4

Re subparagraph 1

Point 1 continues the former Section 14(4)(1).

Re subparagraph 2

Point 2 continues the former Section 14(4)(2).

Re paragraph 5

Paragraph 5 sets out the amount of the respective fines. The previous tier system has been maintained and the levels have been adjusted. The levels are set at 10 and 7 million, (highest), 2 million euro (second stage), 1 million (third stage), EUR 500,000 (fourth stage) and EUR 100,000 (fiveth stage). Requirements set out in Article 34 NIS 2 Directive require modifications in the context of turnover rules.

Re subparagraph 1

Infringements of points 1(d), 2 to 5 and 9 of paragraph 2 shall be classified at the highest level. In these points, breaches of risk management measures and reporting obligations are penalised (maximum level of fines).

Re letter a

Article 34(4) NIS 2 Directive laid down specific requirements for infringements of points 1(d), (2) to (5) and (9) of the NIS 2 Directive: 10 EUR million or at least 2 % of the total worldwide turnover of the undertaking to which the person concerned belongs in the preceding financial year.

Re letter b

For infringements of points 1(d), (2) to (5) and (9) of paragraph 2 in respect of important entities, Article 34(5) of the NIS 2 Directive provides for an amount of EUR 7 million or at least 1.4 % of the total worldwide turnover of the undertaking to which the data subject belongs in the preceding business year.

Re subparagraph 2

The second level (2 million euro) concerns infringements of paragraph 2, point 1(a). No change has been made to the amount of the fine; the reference to Section 30(2), sen-

tence 3 of the OWiG in the old version of Section 14(5) makes it possible to amend it in the form of a tenfold increase.

Re subparagraph 3

At the third level (one million euro) infringements of paragraph 1 and point 10 of paragraph 2 shall be classified: There is no change in the amount of the fine. The previous reference to tSection 30(2), sentence 3 of the OWiG has been taken over.

Re subparagraph 4

The fourth stage was valued at EUR 500,000.

There was no change in this regard for an infringement of paragraph 2 point 1(c) (Section 18). Infringements of supervisory and enforcement measures pursuant to Section 63(3) sentence 1, (6) sentences 1 and 3 and (7) sentences 1 and 3 and (8), both in conjunction with Section 64, were also included at this stage because of their importance.

A breach of paragraph 2, points 6 and 8, was also included at this stage. This is an infringement of the registration obligations.

Infringements of points (11) to (13) of paragraph 2 for non-compliance with the requirements for measures also for Top Level Domain Name Registries and domain name registration service providers are also covered by this classification.

There were no changes in the amount of the fine for an infringement of paragraph 2(14), variant 4.

In the fourth stage, infringements of the new paragraph 2, point 14, variants 1, 2 and 3 were also included. The classification was based on the level of fines under points 14, variant 4 and 15, which, in the previous and current versions, are also set at this level and correspond to the wrong content.

There were no changes to paragraph 4.

Re subparagraph 5

The lowest level was the former EUR 100,000.

There were no changes in the amount of the fine for infringements of points 1(b), (7), (16) and (3) of paragraph 2.

Re paragraph 6

Paragraph 6 establishes the basis provided for in Article 34(4) NIS 2 Directive to impose a fine of at least 2 % of the total worldwide turnover in the preceding business year of the undertaking of which the data subject belongs to particularly important entities, in the event of a breach of risk management measures or reporting obligations.

Re paragraph 7

Paragraph 7 establishes the basis provided for in Article 34(5) of the NIS 2 Directive to impose an administrative fine of at least 1.4 % of the total worldwide turnover in the preceding business year of the undertaking of which the data subject belongs to key entities, in the event of a breach of risk management measures or reporting obligations.

Re paragraph 8

Paragraph 8 clarifies the meaning of the term ‘annual turnover’ used in paragraphs 6 and 7.

Re paragraph 9

Paragraph 9 continues the previous Section 14(6).

Re paragraph 10

Paragraph 10 transposes Article 35(2) of the NIS 2 Directive.

On Appendix 1 (Sectors of particularly important and important institutions)

The Appendix implements Annex I of the NIS 2 Directive.

On the definition of healthcare providers in point 4.1.1: The NIS 2 Directive refers to healthcare providers as defined in Article 3(g) of Directive (EU) 2011/24 of the European Parliament and of the Council (the Patient Mobility Directive) for the categories of institutions to be included in Annex 1, point (5). In accordance with Article 3(3)(a) of that Directive, long-term care institutions whose aim is to support persons in need of assistance in routine, daily work do not fall within the scope of the EU Patient Mobility Directive. Therefore, long-term care institutions are not considered to be healthcare providers within the meaning of this Act.

On Appendix 2 (Sectors of key institutions)

The Appendix implements Annex II of the NIS 2 Directive. The references to NACE Rev. 2 (‘NACE numbers’) in points 3.1.1 and 5.2.1 to 5.6.1 are identical to those of the 2008 classification of economic activities (‘the CPA numbers’).

Re Article 2 (Amendment to the Federal Intelligence Service Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 3 (Amendment to the Security Clearance Regulation)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 4 (Amendment to the Special Fees Regulation of the Federal Ministry of the Interior, Building and Community for individually attributable public services in its area of competence)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 5 (Amendment to the Telecommunications Digital Services Act – Data Protection Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 6 (Amendment to the Gender Equality Elections Regulation)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 7 (Amendment to the Second Act to increase the security of information technology systems)

The evaluation of the remaining provisions of the IT-SIG 2.0, to be carried out by 1 May 2025, is not necessary as a result of the NIS 2 implementation to a large extent. The unchanged provisions are already confirmed by this Act.

Re Article 8 (Amendment to the BSI Certification and Qualification Regulation)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 9 (Amendment to the BSI IT Security Label Ordinance)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 10 (Amendment to the De-Mail Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 11 (Amendment to the E-Government Act)

Deletion of the reference to the BSI Act due to the removal of the provision on the IT Council in the former Section 12 of the BSI Act.

Re Article 12 (Amendment to the Passport Data Acquisition and Transmission Regulation)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 13 (Amendment to the Identity Card Ordinance)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 14 (Amendment to the Whistleblower Protection Act)

These are consequential amendments. The category of digital service providers in the current Section 2(12) is referred to in Annex 1, point 6.1.4. in the particularly important and important entities. (Cloud computing), Annex 2, points 6.1.1 (online marketplaces) and 6.1.2 (online search engines).

To Article 15 (Amendment to the Cash Register Anti-Tampering Ordinance)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 16 (Amendment to the Atomic Energy Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 17 (Amendment to the Energy Industry Act)

Re subparagraph 1

The provision is supplemented, as the safety catalogue to be drawn up by the Federal Network Agency is at least the one required to transpose the NIS 2 Directive in: Section 30 include risk management measures for particularly important entities referred to in the BSI Act.

Re subparagraph 2

Re Section 5c (IT security in plant and network operations, defining competence)

The requirements for IT security of installations and networks, previously laid down in Section 11(1a)-(1g) EnWG, will be moved and extended to the newly introduced Section 5c. This takes into account the fact that safeguards are to be taken to protect against threats to telecommunications and electronic data processing systems not only by operators of energy supply networks, but also by operators of energy installations designated as critical infrastructure under the BSI-KritisV. In addition, the scope is extended to include the particularly important and important entities as defined in the BSI Act to implement Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) in the field of energy. Standardising and bundling cybersecurity-related requirements for all actors active in the energy sector will ensure homogenous compliance with IT security standards, thereby increasing the resilience against IT security incidents of the entities needed for the energy transition.

Re paragraph 1

Paragraph 1 corresponds to the deleted Section 11(1a). In accordance with the Art. 21 2nd &. 1 NIS 2 Directive extends cybersecurity requirements to all telecommunications and data processing systems used by operators to provide their services. The requirements will also be extended to include a requirement to take into account necessary precautions in the procurement of fixed assets and services. These will be taken into account in ensuring the protection of energy supply networks against disruptions and threats to telecommunications and electronic data processing systems. The protection of equipment against attacks already exists at the level of the selection and ordering of components and services, which can have an impact on the security of the systems, in particular due to the progressive digitalisation of the energy system. The arrangements may include, in particular, specific requirements for the certification of equipment and clear manufacturer’s declarations. In addition, Bundesnetzagentur aims to ensure public participation by consulting the operators concerned and their associations in order to better take account of sector-specific requirements. The IT Security Catalogue shall be reviewed every two years for its timeliness. Furthermore, the adequate protection of telecommunications and data processing systems exists only if the requirements of the IT Security Catalogue are met.

The term ‘regulatory authority’ is replaced by ‘Bundesnetzagentur’ in order to ensure uniform wording.

Re paragraph 2

Paragraph 2 corresponds to the deleted Section 11(1b). However, in line with the scope of the NIS 2 Directive, the scope is extended to include the particularly important and important entities resulting from the BSI Act. Same as in Art. 21 2nd &. 1 NIS 2 Directive extends cybersecurity requirements to all telecommunications and data processing systems used by operators to provide their services. The requirements will also be extended to include a requirement to take into account necessary precautions in the procurement of fixed assets and services. These will be taken into account in ensuring the protection of energy installations against disruptions and threats to telecommunications and electronic data processing systems. The protection of equipment against attacks already exists at the level of the selection and ordering of components and services, which can have an impact on the security of the systems, in particular due to the progressive digitalisation of the energy system. The arrangements may include, in particular, specific requirements for the certification of equipment and clear manufacturer's declarations. In addition, Bundesnetzagentur aims to ensure public participation by consulting the operators concerned and their associations in order to better take account of sector-specific requirements. The IT Security Catalogue shall be reviewed every two years for its timeliness. Furthermore, the adequate protection of telecommunications and data processing systems exists only if the requirements of the IT Security Catalogue are met.

The term 'regulatory authority' is replaced by 'Bundesnetzagentur' in order to ensure uniform wording.

Re paragraph 3

Paragraph 3 is intended to implement the Art. 21 of the NIS 2 Directive and introduces requirements for the design of the IT security catalogues. Provisions on intrusion detection systems should also be drawn up in accordance with international standards in the IT security catalogues. As a result, responsibility for verifying the use of attack detection systems is transferred from the Federal Office for Security in Information Technology to the Federal Network Agency.

Paragraphs 1 and 2 broaden the IT security catalogues in line with the NIS 2 Directive and will cover all services provided by operators and not only those necessary for the secure operation of the network or facility. The Federal Network Agency has the power to rank the measures in accordance with proportionality, in particular with regard to the safe operation of the network or installations, and may lay down both higher and lower requirements for IT security measures. As the competent authority, the Federal Network Agency is responsible for monitoring compliance with security requirements and may include provisions in the IT security catalogues for documenting compliance with security requirements, such as security audits, audits and certifications. The Federal Network Agency is therefore empowered to rank in the light of proportionality and to provide for more stringent evidence requirements for the safe operation of the network or installations.

As the scope of paragraph 2 has been extended by operators of critical installations to include particularly important and important entities, the Federal Network Agency will be empowered to provide information on their entry into force in the IT security catalogues. This will ensure an appropriate transition period.

Re paragraph 4

Paragraph 4 restructures the Federal Network Agency's verification of compliance with safety standards. Operators are required to submit documentation of compliance with the safety requirements, in line with the requirements of the BSI Act. If necessary, the Federal Network Agency may require the submission of corrective action plans. This informs the Federal Network Agency of the safety deficiencies identified during the certification procedure. The demonstration shall be used to monitor and verify the measures taken by oper-

ators and thus to ensure an adequate level of safety. In the case of safety deficiencies, the Federal Network Agency may require the safety deficiencies to be remedied. The Federal Network Agency is also entitled to carry out and arrange for on-site inspections to be carried out and to require the submission of documents. These are to be carried out in particular in cases of suspicion.

Re paragraph 5

Paragraph 5 transposes Articles 32 and 33 of the NIS 2 Directive.

Re paragraph 6

Paragraph 6 transposes Article 23 of the NIS 2 Directive.

Re paragraph 7

Paragraph 7 serves to make the reporting system referred to in paragraph 6 efficient. The Federal Office for Information Security will remain the central body for receiving reports on security issues. The role of the Federal Office for Information Security as a ‘centre of expertise’ makes sense in order to pool knowledge and experience as much as possible. Paragraph 5 provides that significant disruptions to the availability, integrity, authenticity and confidentiality of the information technology systems, components or processes which may or have led to a failure or impairment of the functioning of the energy supply network, the relevant energy installation or the digital energy service must continue to be notified immediately to the Federal Office for Information Security. However, according to paragraph 7, the role of the Federal Network Agency in the process is strengthened by forwarding all notifications received to the Federal Office for Security in Information Technology pursuant to paragraph 6 and the BSI Act to the Federal Network Agency without delay if they are relevant for the security of energy supply and the achievement of the objectives under Section 1. The Federal Network Agency will then prepare an energy assessment of the incident in order to extend the BSI safety warning. The aim of such a process is, on the one hand, to better inform energy operators about security incidents and, on the other hand, to assess the impact on the energy sector and thereby enable efficient crisis preparedness and, if necessary, action to be taken. An energy system and economic assessment would reveal links or interactions in the energy system. In addition, the competences of the specialised authorities can be used in a targeted way. In preparing the evaluation, the Federal Network Agency may involve transmission and distribution system operators, which is due to their role and system responsibility (Section 13 and Section 16 EnWG). The involvement of transmission system operators in the evaluation and the resulting dialogue with the industry could concentrate the flow of information and also create confidence. This involvement can be achieved in particular by convening an expert panel composed of representatives of the Federal Office for Information Security, the Federal Network Agency and the transmission system operators. The statutory mandate to carry out a joint assessment by the Federal Office for Security in Information Technology and the Federal Network Agency is also supplemented by an obligation to carry out a final assessment of the IT security incident once it has been remedied.

Re paragraph 8

Paragraph 8 corresponds to the deleted Section 11(1d). Paragraph 8 transposes Article 3 of the NIS 2 Directive.

Re paragraph 12

Paragraph 9 corresponds to the deleted Section 11(1g).

Re subparagraph 3

These are consequential amendments. The remuneration in the Act will be adapted to the above changes.

Re subparagraph 4

These are consequential amendments. The remuneration in the Act will be adapted to the above changes.

Re subparagraph 5

These are consequential amendments. The remuneration in the Act will be adapted to the above changes.

Re subparagraph 6

The incident notification requirement will be recast taking into account the new minimum requirements set out in Article 23 of the NIS-2 Directive.

Re Article 18 (Amendment to the Measurement Point Operation Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 19 (Amendment to the Energy Security Act)

Re subparagraph 1

In so far as the Federal Network Agency, as the competent authority, implements the Act, the current transmission rules are supplemented to the effect that the data obtained by the Federal Network Agency pursuant to Section 1 of the Gas Security Regulation (GasSV) and Section 2a of the Energy Security Act (EnSiG) are made available to Bafin at the request of the Federal Financial Supervisory Authority (Bafin). This is done with strict earmarking of Bafin's statutory tasks. The aim is to enable Bafin, among other things, to identify at an early stage risks to stability, such as for individual entities supervised by the Bafin, as well as the resulting risks to the economy as a whole. For example, in the event of a gas shortage, corporate risks could be transferred to invested banks and thus to the entire financial market. By referring to Section 1 GasSV and Section 2a EnSiG, the scope of the data concerned is clarified. The use of the data obtained must be carried out by the Bafin in accordance with data protection legislation and must be limited to what is necessary for the performance of its tasks.

Re subparagraph 2

These are consequential amendments. The terminology and the reference to the provision of the current BSI Act will be adapted.

Re Article 20 (Amendment to the Heat Planning Act)

These are consequential amendments. The references to provisions of the current BSI Act will be adapted.

Re Article 21 (Amendment to the Fifth Book of the Social Code)

These are consequential amendments. The references to provisions of the current BSI Act will be adapted.

Re Article 22 (Amendment to the Digital Health Applications Regulation)

These are consequential amendments. References to the provisions of the current BSI Act will be adapted.

Re Article 23 (Amendment to the Sixth Book of the Social Security Code)

Re subparagraph 1

Necessary adaptation of the table of contents as a result of the amendment made by this Act.

Re subparagraph 2

The Deutsche Rentenversicherung Bund not only performs its own institutional tasks of the statutory pension insurance scheme, but also the fundamental and cross-cutting tasks for all pension insurance institutions. The federal and regional authorities are represented in the institutions dealing with fundamental and cross-cutting issues.

By extending the statutory catalogue of basic and horizontal tasks of the Deutsche Rentenversicherung Bund to coordinate the information technology of pension insurance, the basis for substantive and organisational measures aimed at strengthening IT security without losing sight of the equivalent objective of cost-effectiveness of action. Co-ordination of information technology also involves taking stock of advances in technical development. The necessary design of the coordination activities follows from Section 146 sentence 1 points 1 to 4. The regulatory concept takes into account the elements put forward by the pension insurance institutions and the Länder side and the binding decisions recently taken by the institutions in the field of IT security. These sub-statutory provisions are confirmed and strengthened by the legislator. The implementation of the substantive and organisational measures remains, unless otherwise specified, within the competence and responsibility of the individual statutory pension insurance institutions. This also applies to tasks in the field of information technology which do not fall within the scope of the new fundamental and horizontal task.

The differentiated responsibilities are intended to prevent, on the one hand, the adoption of important security measures or delays in the event of decentralised responsibility as a result of divergent assessments or misunderstandings, and, on the other hand, decisions on IT security issues which are taken organisationally far from the respective IT facilities lead to undesirable side-effects due to incomplete knowledge of the facts.

Re subparagraph 3

Necessary consequential amendment to insert a new eighth sub-section.

Re subparagraph 4

Re Section 146 (Binding decisions on information technology security)

Section 146 sentence 1 obliges the Deutsche Rentenversicherung Bund to take the binding decisions deemed necessary to strengthen IT security. Information technology and its security are constantly changing. It is the responsibility of the Deutsche Rentenversicherung Bund to make further binding decisions.

The Deutsche Rentenversicherung Bund has taken first steps to strengthen IT security. The deadline set takes this into account.

Re Section 146, sentence 1 subparagraph 1

The Deutsche Rentenversicherung Bund is obliged to lay down uniform principles in the field of information technology and information security, which are binding on all statutory pension insurance institutions. The need to ensure a uniform level of security for all statutory pension insurance institutions, including in the area of information security, is confirmed by its inclusion in the legal text. A uniform level of safety can be achieved through uniform safety standards and security concepts. The principles are minimum requirements which are not intended to remove the responsibility of individual carriers, in particular as operators of critical infrastructure.

The commitment also includes assessing progress in the development of information technology in terms of benefits and feasibility in statutory pension insurance and monitoring and evaluation of risks to information technology.

Re Section 146, sentence 1 subparagraph 2

This addition obliges the Deutsche Rentenversicherung Bund to establish a uniform organisational framework. The establishment of a common data centre was a first step in practice by the statutory pension insurance institutions. In future, the information technology infrastructure of the statutory pension insurance scheme should in principle lie with the Deutsche Rentenversicherung Bund.

Re Section 146, sentence 1 subparagraph 3

The statutory pension insurance institutions also use software applications developed by them to carry out their tasks. Their development is carried out by the IT facilities of various institutions. This makes it more difficult to develop according to uniform standards and dates and has led to the use of incompatible versions of the applications. The development of pension-related applications is therefore to be bundled at the Deutsche Rentenversicherung Bund. The responsibility for the application operation and use of the applications remains with the individual institutions.

Re Section 146, sentence 1 subparagraph 4

By defining a procurement concept, the aim is to increase the standardisation and cost-effectiveness of hardware, software and infrastructure components. This does not have to result in all pension institutions being equipped with uniform products. As long as the devices are compatible with each other, the beams may be equipped with devices of different users.

Re Section 146 sentence 2

In addition to general pension insurance, the Deutsche Rentenversicherung Knappschaft-Bahn-See is also required to carry out other tasks conferred on it by law (e.g. health and care insurance, mini-job-Zentrale, Federal Accessibility Office) and special benefits (e.g. benefit supplement, pension for miners, benefits from the Seemannskasse). These require specific rules. The principles arising from sentence 2, subparagraph 17 and their implementation must safeguard the interests of the interconnected system as a whole and its specific performances and ensure appropriate powers. Therefore, necessary deviations are allowed.

Re Article 24 (Amendment to the Regulation on the Accessibility Enhancement Act)

This is a consequential amendment. The reference to the provision of the current BSI Act has been adapted.

Re Article 25 (Changes to the Eleventh Book of the Social Code)

These are consequential amendments. The references to provisions of the current BSI Act will be adapted.

Re Article 26 (Amendment to the Telecommunications Act)

The existing provisions of the Telecommunications Act (TKG) concerning the cybersecurity of public telecommunications networks will be adapted in line with the requirements of the NIS 2 Directive. In addition, the references to provisions and the terminology used in the current BSI Act are adapted.

Re subparagraph 1

This is a consequential amendment.

Re subparagraph 2

The definitions in Section 3 of the TKG are adapted in the light of the NIS 2 Directive: The already existing definition of an ‘incident’ in Section 3(53) of the TKG is aligned with Article 6(6) of the NIS 2 Directive. Furthermore, in transposing Article 6(1) of the NIS 2 Directive, the definition of a ‘network and information system’ is added.

Re subparagraph 3

The amendments transpose the NIS 2 Directive, which deletes Articles 40 and 41 of Directive (EU) 2018/1972 (cf. Article 43 of the NIS 2 Directive), which are transposed in Sections 165 et seq. of the TKG. The amendments to Section 165 of the TKG transpose Articles 20, 21 and 23 of the NIS 2 Directive. Editorial adjustments are also made.

Re subparagraph 4

These are purely editorial adjustments.

Re subparagraph 5

The amendments to Section 168 of the TKG, which so far transposes Article 40 of Directive (EU) 2018/1972, are intended to transpose Article 23 of the NIS 2 Directive.

Re subparagraphs 6 to 8

These are purely editorial adjustments.

Re Article 27 (Amendment to the Hospital Structure Fund Regulation)

Re subparagraph 1

The scope of the Hospital Structure Fund shall remain unchanged for the remaining duration of the Fund. In order to avoid that future amendments to the BSI Regulation increase the number of hospitals eligible for funding from the Fund to improve their IT security, reference is made to the BSI-Kritisverordnung in its current version for the delimitation of the hospitals concerned. In other respects, these are consequential changes. The reference to the provision of the current BSI Act has been adapted.

Re subparagraph 2

These are consequential amendments. The references to the provisions of the current BSI Act will be adapted.

Re Article 28 (Amendment to the Foreign Trade Regulation)

These are consequential amendments. The references to the provisions of the current BSI Act will be adapted.

Re Article 29 (Amendment to the Trust Services Act)

Pursuant to Article 42 of the NIS 2 Directive, the security and reporting requirements for trust service providers are deleted from Article 19 of Regulation (EU) No 910/2014 (eIDAS). This removes the need to designate a competent body within the meaning of the latter Article. The provisions of the BSI Act will now apply to trust service providers.

Re Article 30 (Further Amendment to the BSI Act)

Article 30 implements the intended postponement of the statutory designation of critical installations into the umbrella law to strengthen the physical resilience of critical installations (KRITIS umbrella law). Article 30 enters into Article 33 only upon the entry into force of a regulation under the KRITIS Common Law. This is a successor regulation to the former BSI Criti Regulation. This ensures that at all times there is only one regulation on the KRITIS provision. Pending the adoption of the ordinance pursuant to Section 5(1) in conjunction with Section 4(3) of the KRITIS-Dachgesetz, this is, on a transitional basis, the statutory ordinance pursuant to: Section 56(4) of the BSI Act. The power to issue a regulation in Section 56(4) BSI Act shall be deleted from the entry into force of the Regulation pursuant to Section 5(1) in conjunction with Section 4(3) of the KRITIS-Dach Act.

Re subparagraph 1

The original definition is replaced by a reference to the definition in the KRITIS Common Act.

Re subparagraph 2

The existing provisions on the designation of operators of critical installations have ceased to exist because of the references in the KRITIS umbrella law.

Re subparagraph 3

The list of sectors covered by the previous Section 2, point 24 The BSI Act is replaced by that of the KRITIS General Act.

Re Point 4 and point 7

The statutory ordinance under the KRITIS General Act replaces the existing BSI-KritisV, and the reference to the regulatory power under the KRITIS Common Act is amended.

Re Article 31 (Further Amendment to the Telecommunications Act)

This Article will also enter into force only upon the entry into force of the successor regulation under the KRITIS Common Law. To the statement of reasons relating to Article 30 reference is made.

Re Article 32 (Further Amendment to the Foreign Trade Regulation)

This Article will also enter into force only upon the entry into force of the successor regulation under the KRITIS Common Law. To the statement of reasons relating to Article 30 reference is made.

Re Article 33 (Entry into force, abrogation)

Re paragraph 1

The date of entry into force shall be the day after its promulgation. Moreover, the content of the NIS 2 Directive that is relevant to the obligations of essential and particularly important entities has already been known since the Commission's draft of December 2020.

Re paragraph 2

Paragraph 2 lays down the temporal link between the postponement of certain provisions to critical installations in: Article 30, which are to be moved to the umbrella law on strengthening the physical resilience of critical facilities (KRITIS umbrella law). The articles following Article 30 contain corresponding consequential amendments.