1. ------IND- 2020 0496 D-- EN- ------ 20200901 --- --- PROJET

Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data

pursuant to
§ 109 of the Telecommunications Act (TKG)
Version 2.0

Publisher:

Federal Network Agency for Electricity, Gas,

Telecommunications, Post and Railways

As at: 29/4/2020

---

*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 of 17 September 2015, p. 1).

Table of contents

1 Systematics, addressee, content and proportionality of the protective measures

The ever-increasing dependence of the economy and society on telecommunications, especially taking into account the comprehensive digitalisation of all areas of daily life, is causing high demands to be placed on the security and availability of telecommunications networks and services.

Against this background, § 109 of the Telecommunications Act [Telekommunikationsgesetz – TKG] defines certain protection objectives and obligations. § 109(1) of the TKG defines the protection of personal data and the protection of telecommunications confidentiality as general protection objectives. It is each service provider's responsibility to pursue these general protection objectives. The special protection objectives according to § 109(2) of the TKG, however, are concerned with the protection of the telecommunications infrastructure from disruptions and risks as well as the availability of telecommunications services. The pursuit of special protection objectives is restricted to the operators of public telecommunication networks and the providers of publicly accessible telecommunication services.

To achieve the protection objectives, all companies must take technical precautions and other measures. In order to pursue the special protection objectives, measures must be taken to protect telecommunications and data processing systems against unauthorised access to minimise the effects of security breaches on users or on interconnected networks. To better control the risks for the telecommunications infrastructure and availability of telecommunications services, § 109(4) of the TKG provides for the creation of security concepts and the appointment of security officers.

The principle of proportionality applies to state requirements. Companies can therefore only be expected to take suitable, necessary and appropriate technical precautions and other measures. In the context of the necessity of a precaution or measure, the state of the art must be taken into account (§ 109(1), sentence 2 TKG; § 109(2), sentence 3 TKG). A precaution or measure is appropriate if the technical and economic effort required for it is not disproportionate to the importance of the telecommunications networks or services to be protected (§ 109(2), sentence 5 TKG).

In fulfilling its obligations under telecommunications law, the company must also observe the general data protection requirements of the Federal Data Protection Act [Bundesdatenschutzgesetz – BDSG] and the General Data Protection Regulation (GDPR). If obligations under § 109 of the TKG are fulfilled by other persons or bodies on behalf of a responsible party and data is processed here, the responsible party in accordance with § 109 of the TKG must ensure compliance with the provisions of telecommunications law. This does not affect the direct data protection responsibility of the commissioned person or body under general data protection law.

2 Function and basic content of the catalogue of security requirements

Operators of public telecommunications networks and providers of publicly accessible telecommunications services must present the technical and organisational protective measures they have taken in a security concept as per § 109(4) of the TKG. The basis for this security concept and for the technical measures and other measures to be taken is the 'Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data according to § 109 of the TKG', which was drawn up by the Federal Network Agency, in agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information.

Fundamental security requirements for the operation of telecommunications and data processing systems and for the processing of personal data are described in Chapter 3. Compliance with these security requirements is mandatory for all companies. Chapter 4 is intended to provide an overview of the relevant legal requirements of the TKG (§§ 88-109). Information on creating a security concept can be found in Chapter 5. Annex 1 describes suitable technical and organisational measures for meeting the requirements for telecommunications service providers with an IP infrastructure. Annex 2 contains additional security requirements. The additional security requirements are aimed at operators of telecommunications networks with an increased risk potential.

Responsibility for the correct and proper implementation of protective measures is always the responsibility of the obliged party. It must ensure that no loss of security is to be expected, even if tasks are transferred to third parties.

According to § 109(7) of the TKG, the Federal Network Agency can order that operators of public telecommunications networks or providers of publicly available telecommunications services undergo a review by a qualified independent body or a competent national authority. The purpose of such a review is to determine whether the requirements of § 109(1) to (3) of the TKG have been met. The catalogue for security requirements can thus also form the basis for the security audit of a qualified independent body in accordance with § 109(7) of the TKG.

Manufacturers, associations of operators of public telecommunications networks and associations of providers of publicly available telecommunications services were involved in the creation of the catalogue.

3 Security requirements for the operation of telecommunications and data processing systems and for the processing of personal data

A holistic concept forms the basis and the starting point for building sustainable security management. Information security management, or IS management for short, is the part of general risk management that is intended to ensure the confidentiality, integrity and availability of information, business processes, applications and IT systems. However, information security is not just a matter of technology. To achieve a level of security for all business processes, information and technology that meets the requirements, suitable organisational and personnel framework conditions must also be created to a considerable extent.

The security requirements listed below address these issues. The requirements apply to all obligated companies and are of a general nature. In this respect, they form the basis of all protective measures to be implemented. The protective measures derived from the security

requirements must also be adequately taken into account in the security concept to be drawn up. The assessment of the appropriateness of a security concept protective measure is initially the responsibility of the obligated company. This is a continuous assessment process in which strategies and measures are constantly checked and adapted to changing requirements. The Federal Network Agency regularly checks compliance with the requirements of the security catalogue and the implementation of the security concept.

The security requirements of this catalogue are therefore neither conclusive nor can they be changed over time. Depending on the criticality of a particular network or service or developments in technology, further requirements may be required in individual cases.

3.1 Organisation

If the obligated company is a merchant or a single-member company, the responsibilities and processes are easy to assign. In many cases, however, the obligation under § 109(1) to (3) of the TKG is based on a business or offer based on a division of labour. The manager of an obligated company based on a division of labour must therefore pay attention to a clear and defined structure and process organisation. This also includes the designation of the security officer in accordance with § 109(4) of the TKG.

3.1.1 Organisational and risk management

Each company must ensure that a binding process is in place to identify risks to networks, services and the processing of personal data. Significant threats (security risks) that have been identified for networks, services and data must be documented. Recognised residual risks are to be checked while taking proportionality into account.

3.1.2 Security roles and responsibilities

Personnel responsibility must be defined for the security of information, business processes, applications, tasks and regulations. All employees must be informed of these responsibilities in a suitable manner. There must be an indication of when and how security officers are to be involved.

- When assigning the respective security roles, an instrument of appointment can provide clarity, transparency and openness. In this context, tasks and powers could also be defined.

- Designation alone is not sufficient. It must be possible to reach the persons responsible for security incidents in the performance of their roles. The creation of representation rules is an important prerequisite in this context.
- Safety expertise becomes outdated with time. The designated personnel must therefore be trained on a regular basis.

3.1.3 Supplier management

Telecommunication services can often only be provided with recourse to third parties. Suppliers and vicarious agents play an important role against this background. The obligated company must therefore assess the reliability, trustworthiness and quality of the vicarious agent or supplier. It must be ensured that dependencies on third parties do not impair the security of networks or services as well as personal data. The following must be observed in this context:

- The reliability of the third party can only be assessed on the basis of suitable information. Therefore: Information must be obtained before commissioning.
- Third parties are to be bound by contract. It must be ensured here that security requirements are included in the contractual basis along with providers (e.g. when IT products are purchased or IT services are used). Particular care should be taken in this regard if entire business processes (help desks, call centres, network connections) are outsourced.
- The third party must act in accordance with data protection law. This can be achieved through appropriate contractual arrangements. When orders are processed, the provisions of Article 28 GDPR must be observed.
- The security requirements should not only be defined and updated, but their compliance should also be monitored if possible. This must always be done while orders are processed. The monitoring should be repeated on a regular basis.

3.2 Security in personnel management

Employees make a significant contribution to compliance with the protection objectives mentioned at the beginning. Elaborate protective measures and technical redundancy concepts only bring about the desired success if the employees also do not represent a security gap in the company and are aware of their responsibility for their security-related activities. This chapter covers the security requirements for the HR department, the management and the personnel in the company. This also includes personnel who are provided externally to perform certain tasks (e.g. by suppliers or manufacturers).

The following requirements must be taken into account before being hired and also after leaving the company.

3.2.1 Security check

Depending on the task and responsibility, an appropriate security check may be required. With regard to employees and contractors, it is advisable to validate their identity and professional references, especially for those with security-related tasks and responsibilities (e.g. system administrators, security officers or security guards). The checking procedure used should be documented.

The company should ask employees to present their identity card in order to clearly establish their identity. Other suitable evidence may include certified certificate copies, personal certificates or an official certificate of good conduct. It may be a appropriate to get additional references from previous employers.

3.2.2 Security expertise and awareness

The personnel must have suitable and relevant security expertise and develop an awareness of how to handle sensitive data.

It must therefore be ensured that the staff employed and commissioned have taken suitable and relevant training and that material on security issues is made available. The attendance of the training must be documented.

Knowledge becomes outdated with time. Regular training measures and awareness sessions for employed and commissioned personnel regarding the relevant security issues (e.g. data protection, telecommunications confidentiality) should therefore be implemented.

Training content should also be checked on a regular basis, taking changes into account, and updated if necessary.

3.2.3 Personnel changes

Changing personnel is associated with security risks. The company must therefore observe certain security requirements if employees change their area of responsibility, leave the company or new employees are trained:

- Regulations for the administration of personnel changes or changes in responsibilities must be observed.

- After a change in personnel or agents, access rights to corresponding systems, buildings or facilities must be adapted or blocked immediately. Passwords that have been issued are to be managed according to the state of the art.
- New personnel must be informed and made aware about the applicable guidelines and procedures.

3.2.4 Dealing with violations

Binding rules should be laid down on how to deal with security breaches due to violations by a company's own employees.

3.3 Security of data, systems and facilities

This chapter covers the physical and logical security of data, network and information systems to protect basic values (confidentiality, availability and integrity).

3.3.1 Secure handling of sensitive data and information

In the field of telecommunications, the protection of inventory data and especially of highly sensitive data such as traffic, tax or content data must be guaranteed. They are subject to data protection requirements and requirements for the protection of telecommunications confidentiality. Regulations for the secure handling of such data and information must therefore be laid down. In particular:

- Sensitive files or documents must be kept under lock and key. Lockable filing cabinets and locked offices should be considered as possible measures.
- Mobile end devices or removable media should be protected with suitable encryption technologies. (MDM) Mobile Device Management should be used.
- Regulations should be laid down for the safe disposal of removable media that are defective or no longer required.
- Hard drives with sensitive data must be disposed of in such a way that the data can no longer be restored.

3.3.2 Physical and elementary protection requirements

A security risk is also posed by vandalism, theft, fire, water, dust or natural hazards. Appropriate physical protective measures should be taken to ward off security risks of this type as far as possible so that the availability of the network and service is maintained. This includes at least the following measures:

- Physical security elements must be defined that prevent unauthorised access, damage to and impairment of information and information processing facilities (e.g. by means of security locks, motion detectors, intrusion detection systems or video surveillance).
- Security areas should be protected by adequate access control.
- Devices and equipment must be serviced at regular intervals or at intervals recommended by the manufacturer.
- Telecommunications cabling and power cabling must be adequately protected against interruptions, interference and damage. Redundant lines must be laid separately from each other. Cables should be laid underground and protected by pipes as well as locked rooms and closets.
- Water-carrying pipes should be avoided in server rooms.
- Measures to protect against natural disasters and accidents must be taken.
- An assessment of the effectiveness of physical and environmental protective measures must be carried out on a regular basis.
- The use of fire, gas and smoke detectors or extinguishing systems should be appropriate to the size of the premises and should be maintained regularly.
- Compliance with the fire protection regulations must be checked regularly.

3.3.3 Security of supply (availability of the overall system)

An important component in the area of publicly accessible telecommunications is ensuring security of supply (telecommunications, electricity, air conditioning, etc.). The following protective measures must be taken:

- Devices and equipment must be protected against power failures and other disruptions.
- Redundant lines should be available via different supply routes.
- Adequate dimensioning of the air conditioning and power supply must be determined and monitored regularly.
- Switchgear, emergency generators, batteries, etc. must be checked regularly and, if possible, tested.

- A procedure for the implementation of security-critical supplies, utilities and support facilities must be created.
- Measures to protect the supply and provision of the utilities are to be implemented.

3.3.4 Control of access to network and information systems

Without suitable mechanisms for access control, it is not possible to prevent unauthorised use of telecommunications devices and telecommunications systems. Unauthorised persons can also access confidential information, make manipulations or cause interference. Appropriate authorisations are intended to control and manage access to information.

Possible protective measures include the following:

- Users have unique identifiers and are authenticated before they can access services or systems.
- Passwords may only be saved in an encrypted form.
- Roles, rights, responsibilities and procedures for assigning and revoking access rights must be defined.
- Access to network and information systems must be logged. Deviations from this procedure must be recorded and logged.
- Remote maintenance access must be adequately secured (dedicated VPN access).
- External parties are only allowed to be in secure areas if they are accompanied or after a suitable security check and instruction. External parties are people from external companies, for example in cases of maintenance work, conversions or cleaning work.
- The access control mechanisms are checked regularly and adapted if necessary.
- It must be ensured that only authorised persons have access to secure technical systems.

3.3.5 Integrity and availability of network and information systems

The integrity and availability of network and information systems and the protection against viruses, code injections and other malware that can change the functionality of systems must be ensured:

- It must be ensured that software for network and information systems is not manipulated or changed without authorisation (e.g. by means of unauthorised

configuration changes). Changes should be documented. Instances of unauthorised access must be detected. Systems and applications should always receive the latest security updates.

- Appropriate malware detection measures must be implemented.
- Measures to raise employee awareness should exist and be implemented.
- It must be ensured that security-critical data (such as passwords, shared secret keys, private keys, etc.) are not disclosed or manipulated.
- The effectiveness of measures for protecting the integrity of systems should be checked and evaluated.
- Passwords should be securely authenticated and, if necessary, changed.
- Training should give employees the ability to identify suspicious emails or links.

3.3.6 Confidentiality of communication

The confidentiality and integrity of communication content and metadata must be guaranteed:

- Appropriate encryption methods should be used to ensure adequate protection of the confidentiality of communication content and metadata.
- Suitable authentication mechanisms for customer and service networks must be implemented.
- The use of networks and services should be continuously probed for anomalies in an appropriate manner.
- Standardised transmission procedures and measures should be used.
- Customer security-critical data must be especially well-protected (e.g. SIM card data, IMEI number, passwords).
- The effectiveness of methods for protecting the confidentiality of communication content and metadata should also be continuously assessed in an appropriate manner. Location data such as cell IDs are also part of the metadata and are subject to additional requirements (see Section 4.2.4). A cross-check or a (stress) test is an example of a suitable assessment.

3.4 Management

The responsible company management team must ensure proper and secure operation. The following security requirements relate to the operational procedure, change management and the handling of company values.

3.4.1 Operational procedures

Appropriate operational procedures must be used to ensure that the information and communication technology of the relevant obligated company works properly, securely and continuously.

- To be able to ensure this, the operational procedure must be defined and documented as a minimum. Responsibilities for the operation of critical systems must also be assigned to a responsible body.
- Available and necessary resources must be known. Resources in this sense include, among other things, the necessary and actual personnel, systems, applications and premises.
- Available and necessary resources must be constantly checked and, if necessary, managed in an appropriate form.

3.4.2 Change management

Changes may pose security risks. Rapidly changing and constantly increasing user requirements also lead to ever shorter change intervals, including adjustments to system configurations. In this respect, companies may be faced with the task of having to update telecommunications components promptly and reliably, as required. Security practice shows that risks or operational disruptions are often due to incorrect or hasty change management or a lack of a suitable one. To avoid malfunctions or security incidents, changes to network and information systems, infrastructure, documentation, processes, procedures and operations should therefore be planned, monitored, controlled and checked after completion.

- Changes to critical systems should be based on pre-defined and suitably documented procedures.
- An assessment of all potential direct and indirect effects should be carried out.
- Significant actual changes should be logged in an appropriate form.
- The functionality of the telecommunications systems should be checked in appropriate form after changes. All data subjects should be informed of the necessary change details. Any abnormalities identified should be reported to the previously specified body immediately.
- Preventive control measures are recommended, e.g. the four eyes principle.

3.4.3 Asset management

Security requires knowledge. At they very least, the essential facilities, systems and equipment required for the respective network operation or the range of services should be

clearly identifiable. Appropriate inventory and management of facilities and systems can ensure this in individual cases. The administration should also include the configuration control of the essential network and communication systems.

3.5 Malfunctions and security incidents

The detection of, reaction to and reporting of malfunctions and security incidents are dealt with. Security incidents can be triggered by a single event or a chain of different circumstances. Security incidents can cause the confidentiality, integrity, availability or authenticity of information and telecommunications systems to become compromised.

3.5.1 Detection of security incidents and malfunctions

A procedure for identifying security incidents and malfunctions must be set up and checked regularly.

For this purpose, for example, predefined operating parameters such as climate, electricity and data traffic in telecommunications are to be monitored and an alarm must be raised in the event of a security incident or faults.

After malfunctions and/or incidents become known, any affected systems should be adapted and/or improved so that this problem is prevented in the future.

3.5.2 Dealing with security incidents and malfunctions

A security incident can have a singular or multicausal origin. Any type of security incident can cause the confidentiality, integrity or availability of information and telecommunications systems to become compromised. The obligated companies must therefore implement a procedure for defining and handling any kind of security incident, including reporting it to responsible persons and authorities. Regular checks should be carried out to determine whether the specified procedure corresponds to the current circumstances and whether the actual implementation is in accordance with the planning.

- Suitable personnel must be available and appointed in the event of security incidents. In the event of a security breach, it may be necessary to take security measures or make security-related decisions under time pressure or atypical circumstances. The personnel should therefore not only be trained to identify security incidents, but also taught how to specifically handle them.

- —The criticality of the respective disruption or security breach must be assessed in an appropriate form. The reporting channel specified for the evaluation result must then be implemented.
- Critical security incidents must always be investigated. The investigation and results must be documented in a report. The report should indicate which measures have been taken or planned to avoid similar security incidents and their effects in the future or to minimise the security risk. The measures taken or planned in this regard should be justified. If there are significant security breaches in accordance with § 109(5) of the TKG, these must be reported immediately to the Federal Network Agency and the Federal Office for Information Security.

3.5.3 Communication and reporting of security incidents

Adequate security incident reporting procedures should be in place to minimise security incident damage.

- A security incident may trigger a statutory reporting obligation (e.g. §§ 109(5), 109a(1) TKG or Article 33 GDPR). If necessary, current or past security events must be reported to third parties, customers and/or authorities.
- In order to ensure compliance with any reporting obligations as well as the communication and reporting of security incidents, suitable regulations should be implemented in business operations.
- In the event of an attack on passwords, any customers affected must be informed as soon as possible. A suitable notification procedure should be established to ensure this.

3.6 Emergency or failure management

A malfunction or a security incident may lead to failure of the service or network operation. A suitable prevention strategy should take developments of this type into account and develop appropriate defence concepts tailored to each individual case. In this context, it is not only necessary to regulate the technical aspects for maintaining the services. Organisational measures must also be planned and defined in advance and continuously checked. This chapter includes requirements for restoring and maintaining operationally relevant infrastructures.

3.6.1 Maintenance of telecommunications infrastructures and services (business continuity management)

Regulations for maintaining infrastructures and services must contain general instructions and, if possible, specific emergency measures adapted to each individual case. Relevant contact information should be described in an emergency manual and always be up to date. Access to these rules and this information should be ensured.

- The availability of adequate redundancies at the system and service level must be ensured in advance.
- These redundancies must be tested or switched over at regular intervals if this is possible without interruption.
- Critical systems and data must be backed up on a regular basis. Attention must be paid to the statutory deletion and storage periods. In particular, the storage time of the backups should be proportionate to the storage time of the personal data.
- Adapted emergency plans for the operation of critical systems are to be drawn up, defined and implemented. These plans should be evaluated on a regular basis.
- A suitable emergency officer must be appointed. He or she should be familiar with and manage all emergency management activities.

3.6.2 Restart after failures (disaster recovery management)

The downtimes until the network and communication services are functional again must be kept as short as possible with adequate means.

- Appropriate policies and procedures must be developed and established to restore important network and communication services as quickly as possible. These policies and procedures should be evaluated at regular intervals.
- The most important business processes should be prioritised for the restart.
- Supplier contracts should be checked in advance for a replacement provision.
- One possible suitable protective measure is the provision of suitable replacement devices for infrastructure and telecommunications systems.
- Another possible suitable protective measure is also the provision of suitable, mobile network backup systems in individual cases.
- Setting up emergency workplaces preventively may be useful for maintaining services.

3.7 Monitoring and testing procedures

Monitoring and test procedures should be introduced to make systems and processes as secure as possible and to continually optimise them. Requirements for monitoring and logging important network and communication systems are described below.

3.7.1 Monitoring and logging measures

Business and security-related events should be logged. Logging data is used to evaluate and monitor certain events. Detailed and continuous logging that is automated to the greatest possible extent can increase the evaluation options. In a best-case scenario, the logging data permits a suitable security analysis based on a forensic examination. All security-relevant events must therefore be logged and stored in an evaluable form. If data is no longer required for these purposes, they must be deleted immediately.

- A set of rules for monitoring and logging operationally relevant systems that is adapted to each individual case should be introduced and implemented. The rules should be evaluated on a regular basis.
- The automatic monitoring and logging of operationally relevant systems may allow additional information suitable for evaluation to be obtained in individual cases.
- Administrative activities or work on operationally relevant systems should be logged.

3.7.2 Emergency exercises

Chapter 3.6 covered requirements for maintaining and restarting infrastructures and services after emergencies. Emergency exercises should be carried out regularly so that emergency plans and procedures can be implemented as planned in stressful situations. Therefore, a procedure for testing and practising contingency plans to maintain and restore critical services and infrastructures should be established. If possible and necessary, this should also be done in cooperation with third parties.

Scenarios that are as different and realistic as possible should be considered. It should be determined whether planned downtimes are not exceeded and whether the designated crisis management team performs its tasks in practice.

3.7.3 Testing network and IT systems

Changes to or development work on existing network or IT systems are possible risk factors. Regulations for approving and testing network and IT systems should therefore be laid down in advance.

- Network or IT systems should be tested in separate test environments before they are used or connected to existing systems. The same should also take place in the case of adjustments or, for example, after updates.
- Operational systems should be subjected to regular security tests. This applies in particular when new systems are introduced and changes are made.
- It must be ensured that tests have no impact on the security of networks and services. The use of sensitive data must be avoided.

3.8 Assessment of security measures

All safety measures must take the state of the art into account. However, technology continues to evolve. In addition to this, the threat situation is subject to constant change. Against this background, the security measures taken must be regularly reassessed by the obligated company. An appropriate strategy should therefore be drawn up to assess the security measures taken in each individual case.

- As a minimum, regulations should be drawn up to assess the protective measures taken.
- Regular risk analyses and surveys of defined key figures (e.g. malfunction times and downtimes as an indicator) can be used to assess the security measures.
- Regular and realistic stress tests can potentially identify new risk factors.

3.9 Compliance with legal requirements

Compliance with legal, contractual or voluntary rules must be ensured. For this purpose, a monitoring system should be implemented in operational processes and a responsible body should be designated. Law, like technology or threats, is also subject to constant change. Legal developments should therefore be continuously and appropriately monitored and the applicability thereof to each individual case should be examined. Below, Chapter 4 provides an overview of the relevant statutory provisions of the TKG.

4 Legal security requirements from area-specific regulations

The technical precautions and other measures to be taken in accordance with § 109(1) and (2) of the TKG are aimed at the protection of personal data, telecommunications

confidentiality and the protection of telecommunications infrastructure and the availability of services. These legal interests are not the sole subject matter of the TKG. In this respect, the obligated company may also have to observe other European, constitutional or national regulations.

The following deals exclusively with the area-specific legal requirements of the TKG. For example, regulations for the protection of telecommunications confidentiality can be found in §§ 88 et seq. of the TKG. §§ 91 et seq. of the TKG govern the protection of personal data. The subject matter of §§ 100, 109(5) of the TKG is the protection of the telecommunications infrastructure from disruptions and the availability of telecommunications services.

Union law requirements, changing security situations and technical developments result in the continuous amendment of the TKG. To comply with their legal obligations, the obligated companies are therefore generally required to monitor the development of the relevant legislation and case law and to examine their applicability to individual cases. In this respect, the following information can only provide an area-specific and current overview of the requirements to be met.

4.1 Security requirements for the protection of telecommunications confidentiality (§ 88 TKG)

§ 88 of the TKG is the simple legal expression of the constitutionally enshrined protection of telecommunications confidentiality under Article 10(1) of the Basic Law. The law takes account of the fact that, with the liberalisation of the telecommunications market, telecommunications services are provided by private individuals who are often subject to an indirect and therefore only relative commitment to fundamental rights. Against this background, there was a need to supplement the constitutional protection under Article 10(1) of the Basic Law with a regulation on a non-constitutional level and to thereby hold both private providers and the public authorities directly bound to Article 10(1) of the Basic Law liable.

The confidentiality of the use of the technical medium used to transmit messages is protected by Article 10 of the Basic Law. If communicative data is taken note of, recorded, used or passed on by the state without consent, this constitutes an infringement of fundamental rights. Because of the harmony with § 88 of the TKG, this provision also has a

similar content. In contrast to Article 10 of the Basic Law, the protection is not against the state, but against service providers.
In line with the constitutional case-law on Article 10(1) of the Basic Law, § 88(1) of the TKG also covers the particular circumstances of telecommunications. This includes all the information about times and places as well as the modality of the non-physical communication process, insofar as they may jeopardise the confidentiality of the communication process.

With regard to compliance with security requirements to protect telecommunications confidentiality, the following should be pointed out:

- Each service provider is obliged to preserve telecommunications secrecy. The obligation to maintain secrecy continues even after the end of the activity.
- Service providers must be prevented from obtaining knowledge, for their own benefit or that of others, of the content or the more detailed circumstances surrounding the telecommunication over and above what is necessary for the commercial provision of telecommunications services, including the safeguarding of their technical systems.
- Likewise, unauthorised third parties must be prevented from obtaining knowledge of the content or the particular circumstances of telecommunications.
- Technical equipment for the direct and indirect transmission of message content must also be taken into account, as well as equipment for the collection, processing and use of traffic data (e.g. subscriber line, network termination point, switching and routing equipment, connection network as well as billing or fraud systems).
- In the area of the administration and safekeeping of files that are subject to telecommunications secrecy, storage containers suitable for data protection must be used and corresponding rooms with access control should be utilised sensibly.
- Only persons who have received sufficient instruction about the sensitivity of this data may have access.
- It must be ensured that, in message transmission systems with intermediate storage, only the subscribers determine the content, scope and type of processing through their consent. Protective measures that only allow the subscriber to decide who may enter and access message content can be implemented using appropriate access codes and passwords. These are communicated confidentially only to the subscribers and are to be changed by them independently upon receipt. It is within the participants' freedom of consent to determine to whom they will pass the access codes.

- An example of a possible protective measure against unjustified deletion of message content by the service provider contrary to the contractual relationship is the creation of backup systems.

4.2 Security requirements for the protection of personal data (§§ 91 et seq. TKG)

Section 2 of Part 7 of the TKG regulates area-specific data protection. General data protection regulations of the General Data Protection Regulation (GDPR) and the other regulations of the BDSG also apply.

It can be stated that the GDPR does not impose any additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communication services in public communication networks if they are subjected to special obligations laid down in Directive 2002/58/EC (ePrivacy Directive) that pursue the same goal (Article 95 GDPR). Accordingly, the provisions of the GDPR apply primarily, unless there is conflicting regulation of the TKG in implementing the ePrivacy Directive. § 95 of the TKG will therefore be largely superseded by the GDPR, for example: Because, with a few exceptions, the ePrivacy Directive does not contain any regulations on inventory data processing. The only exceptions to this are § 95(2), sentences 2 and 3 of the TKG as an implementation of Article 13(2) of the ePrivacy Directive. Corresponding comments have therefore not been given below.

§ 109 of the TKG, on the other hand, constitutes an implementation of Article 4(1) of the ePrivacy Directive as well as Directive 2002/21/EC (Framework Directive) and is therefore primarily applicable.

4.2.1 Information obligations (§ 93 TKG)

The information obligations are to safeguard the exercise of the right to informational self-determination because

‘*Those who cannot understand with sufficient certainty what information related to them is known to certain segments of their social environment, and who are not able to assess to a certain degree the knowledge of possible communication partners, can be hindered significantly in their freedom to plan or make decisions based on their own self-determination. The right to informational self-determination would not be compatible with a*

social order and a legal order that enables it in which citizens can no longer know who has knowledge of what, when and on what occasion.' (BVerfGE 1, 44)
These grounds given by the Federal Constitutional Court also make it clear that constitutional protection cannot be limited to intervention by the state, but, for example, must also include that by private telecommunications companies.

The collection, processing and use of inventory and traffic data by the obligated telecommunications companies can be carried out, among other things, in 'customer care and billing systems', in 'fraud systems (§ 100(3) TKG)', in 'systems for notification of incoming connections (§ 101 TKG)' or in 'systems for inclusion in public telephone directories' (§ 45m TKG).

With regard to the observance of data protection law information obligations, Article 13 of the GDPR and § 93 of the TKG must be observed. The following measures must also be taken in this regard:

- It is recommended that employees be made aware of data protection issues by taking appropriate instructional measures. In addition, a contractual commitment to respect data protection should be made by all employees involved.
- When the contract is concluded, subscribers must be given the name and contact information of the data controller. The subscribers are to be generally informed about what type of data is to be processed for what purposes and on what legal basis. The recipients or categories of recipients to whom the personal data of the subscribers are transmitted must also be named. If a transfer to a third country, that is, a country outside the EU and the European Economic Area, is intended, this must also be indicated to the subscribers. To ensure that data subjects know who the correct contact person in the company is for data protection matters, the contact details of the company data protection officer must also be provided. Furthermore, existing data subject rights – such as the right to rectification or erasure – and the right to lodge a complaint with the responsible data protection authority must be pointed out. The subscribers should be made aware of the permissible choice and design options (e.g. use of the inventory data to advise the subscribers, to advertise offers, to carry out market research (§ 95(2) TKG), provision of an itemised bill (§ 99(1) TKG), notification of connections settled as a lump sum (§ 99(1) TKG), entry in the subscriber directory (§ 104 TKG) and provision of information (§ 105 TKG)).
- The subscribers are to be informed about any special risks of breach of network security and, if necessary, also about possible remedies.

4.2.2 Traffic data (§ 96 TKG)

Both traffic data and inventory data are to be considered as personal data. In contrast to inventory data, traffic data is subject to the special protection of Article 10 of the Basic Law or § 88 of the TKG.

The provision regulates collection and use in accordance with data protection regulations and, at the same time, specifies the admissibility requirements for the obligated companies.
These include the following:

- The collection of traffic data can only be permitted if it is necessary for one of the purposes mentioned in Section 2 of Part 7 of the TKG.
- Under certain additional conditions, the determination of the communication profiles of individual subscribers and the analysis of traffic flows may be permitted, § 96(3), sentence 1 TKG.
- As a rule, the service provider must erase the traffic data immediately after the connection is terminated, § 96(1), sentence 3 TKG. Reference is made to the guidelines of the BfDI and the BNetzA for data protection-compliant storage of traffic data (as at 19 December 2012) (available at www.bundesnetzagentur.de).

4.2.3 Determination of charges and billing (§ 97 TKG)

Traffic data generally forms the basis for data processing facts in connection with the determination of charges and billing. In this respect, the provision is an area-specific permission to use traffic data (§ 96(1) TKG, see above).
In this regard, the following should be noted:

- If third parties are involved in the preparation of telecommunications bills or the provision of telecommunications services (e.g. by service providers without their own network infrastructure), then the technical and organisational interface relationships between the client (service provider) and the contractor (vicarious agent) must be clearly regulated.
- Data that is not required in accordance with § 97(3) TKG must be erased immediately.

4.2.4 Location data (§ 98 TKG)

Location data (§ 3, subparagraph 19 TKG) can be merged into motion profiles, which allow conclusions to be drawn about social relationships or habits. Location data therefore has particularly high relevance in terms of data protection law.

- Location data used in relation to the users of public telecommunications networks or publicly accessible telecommunications services may only be processed to the extent required to provide services with additional benefits and within the time period required for this if they have been anonymised or if the subscriber has granted his or her consent to the provider of the service with additional benefits.
- A process must be designed in order to allow the user to temporarily prohibit location data from being processed each time a connection to the network is established or in each case of transmission in a simple manner and free of charge.
- The transmission of location data for the phone numbers under § 98(3) of the TKG (emergency numbers 112 or 110 or the numbers 124 124 and 116 117) must be ensured.
- It must be ensured that the processing of location data is limited to the necessary extent.

4.2.5 Itemised bill (§ 99 TKG)

The subscriber is informed of the details of the billed telecommunication services by means of an itemised bill (EVN). The itemised bill is therefore used for control purposes. However, the itemised bill must be prepared regularly on the basis of traffic data. As this data is subject to telecommunications secrecy, special data protection regulations are to be observed in this context (§ 99(1) TKG). This applies in particular if certain rights of the co-users of a telephone connection are affected (§ 99(2) TKG).
With regard to § 99 of the TKG, the following is pointed out:

- Subscribers are only to be informed of the stored data of those connections for which they are liable to pay if they have requested an itemised bill in text form prior to the relevant billing period. The data of flat-rate connections may only be communicated to them on request.
- The itemised bill is to be made available at the subscriber’s request.
- After requesting an itemised bill, the subscriber must be given the option of receiving the selected phone numbers in a complete form or with the last three digits removed.
- If the itemised bill is sent electronically, measures must be taken to protect telecommunications secrecy and personal data.

- Regulations for the obligated party must ensure that the connections cannot be recognised in the itemised bill in accordance with § 99(2) of the TKG. The unrecognisability of the connections is ensured if the connection is not shown in the itemised bill.
- The obligated company is to retrieve the list of protected advice centres pursuant to § 99(2), sentence 4 of the TKG from the Federal Network Agency on a quarterly basis in an automated process.
- The obliging company must take changes into account in the billing process immediately.

4.2.6 Notification of incoming connections (§ 101 TKG)

In certain cases, the provision grants the subscriber the right to be notified of incoming calls (malicious caller identification procedure) according to a prescribed procedure. Due to the legal structure of this malicious caller identification procedure, subscribers are to be given the opportunity to receive information about the connection making the calls in the event of threatening or annoying calls. The procedure is especially worth considering for suppressed numbers and is often the only way for those affected to take promising legal steps. Please refer to the legal text for details.

The Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information are to be informed immediately of the introduction and modification of the procedure for ensuring the malicious caller identification procedure.

4.2.7 Automatic call forwarding (§ 103 TKG)

The purpose of the provision is to protect subscribers against unwanted forwarding of calls to their connection for a third party. However, the protection requirement is subject to the reservation of technical feasibility.

4.2.8 Message transmission systems with intermediate storage (§ 107 TKG)

Some service providers offer customers the option of storing certain telecommunications content for later use. In this respect, message transmission systems are not used in real time. However, storing telecommunications content can also present a significant risk to personal data and telecommunications secrecy. The aim of § 107 of the TKG is to counter this risk. In this respect, the following is pointed out:

- Intermediate storage providers must ensure that only the subscriber determines the content, scope and type of processing.
- Service providers must take the necessary technical and organisational measures to prevent faulty transmissions and the unauthorised disclosure of message content within their company or to third parties.

4.3 Security requirements for protecting the telecommunications infrastructure and the availability of telecommunications services

4.3.1 Faults in telecommunications systems and misuse of telecommunications services (§ 100 TKG)

The service provider may collect and use inventory, traffic and control data to the extent necessary to identify, limit or remedy faults. In this respect, § 100(1) of the TKG standardises permission granted under data protection law. In certain cases, this is linked to a reporting obligation. General information on the reporting obligation pursuant to § 100(1) of the TKG and its validity can be found at www.bundesnetzagentur.de.

To identify and limit faults, the operator of a telecommunications system is also allowed to connect to existing connections under strict conditions. Any recordings that may have been made must be deleted immediately. This data protection intervention involves an obligation to provide information to the company data protection officer (see as a whole § 100(2) of the TKG).

If there are indications of theft of services or fraud, the service provider can use inventory and traffic data to secure its claim under certain conditions. In this context, information requirements vis-à-vis the Federal Network Agency and the Federal Commissioner for Data Protection must be observed.

4.3.2 Significant security breaches (§ 109(5) TKG)

Network operators and service providers must immediately notify the Federal Network Agency and the Federal Office for Information Security about both actual and possible significant security breaches. Reference is made to the currently valid implementation concept for reporting incidents (as at: 10/11/2017, version: 4.0, OJ BNetzA No 22 v. 11/22/2017).

4.3.3 Data and information security (§ 109a TKG)

The provision regulates certain information requirements in the event of a violation of the protection of personal data (‘data protection breach’ or ‘security breach’). In this context, the obligated company has certain notification obligations towards the data subject, but also towards the Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information. Reference is made to the information from the Federal Network Agency, which is available at www.bundesnetzagentur.de (‘Notification requirements in the event of a breach of the protection of personal data’).

If IT security violations originate from a user-operated data processing system, the obligated company is obligated to provide information to the user under § 109a(4) of the TKG. Through redirection within their own networks, the obligated company is given the opportunity to first identify the user concerned and then enable him or her to remedy the problem (this is referred to as ‘sinkholing’).

An individual examination of the technology or individual consultation from the provider is not required. If it is not technically possible to notify the users concerned within a few days, the providers will only be able to inform their participants and point out aids.

The wording ‘as far as he or she is already aware of it’ makes it clear that to identify users, only traffic data that the company has already collected and stored due to other regulations may be accessed. The collection of further data solely for the purpose of carrying out a notification is therefore not permitted (BT-Drs. 18/4096, p. 37).

§ 109a(5) of the TKG allows the data traffic to be restricted, redirected or stopped in the event of a fault. In view of the increasing number of IT security incidents, these powers should enable them to be remedied, in particular if a user whose systems are causing the fault cannot remedy it or an immediate remedy is not expected and an intervention in the use of the telecommunications service is required in order to remedy or prevent the impairment despite the information being provided.

The obligated company can also restrict or stop data traffic to sources of faults in accordance with § 109a(6) of the TKG in order to counteract the occurrence of faults in the users' telecommunications and data processing systems. This power was given to obligated companies because attackers generally use modular attack tools to infect telecommunications and data processing systems (BT-Drs. 18/11808, p. 11).

5 Implementation of security requirements

§ 109(4) of the TKG lays down different obligations for operators of public telecommunications networks and providers of publicly accessible telecommunications services that have to be fulfilled in different stages. Basically, there is an obligation for both network operators and service providers to create a security concept. A security officer must also be appointed by both. The law only requires the network operator to submit the security concept to the Federal Network Agency upon commencement of operations. The service provider is not legally obliged to submit one. However, it may be obliged to do so by the Federal Network Agency. In addition to these preparation, designation and submission obligations, there is also a declaration obligation. It relates to the actual implementation of the security concept considerations. If the circumstances change, the law requires the company in question to adjust.

The security concept obligations according to § 109(4) of the TKG serve to identify and structure suitable and appropriate measures to protect telecommunications secrecy, data protection and the functionality of networks and services. This catalogue for security requirements is a guideline for fulfilling these obligations.

The Federal Network Agency checks the submission and also regularly checks the implementation of the corporate security concept. If it identifies a security deficiency in this context, it can demand that the identified deficiency be remedied. This must be distinguished from the review by a qualified independent body in accordance with § 109(7) of the TKG. This review does not focus on the company's security concept or its implementation. The subject of this investigation is solely the question of whether the security requirements from § 109(1) to (3) of the TKG are met in individual cases. The review pursuant to § 109(7) of the TKG should therefore compare the company's security assessment with a third party. Catalogue content must also be used for this check. The catalogue is therefore a basis for both action and review.

5.1 Implementation of security requirements

The law specifies a certain content for the security concept. Specifically, this laid down in § 109(4)(1) to (3) of the TKG: In this respect, the concept must include a descriptive report (§ 109(4)(1) TKG), a risk analysis (§ 109(4)(2) TKG) and the corresponding protective measures (§ 109(4)(3) TKG). The basics of the practical implementation of these requirements will be discussed below.

5.1.1 Description of the public telecommunications networks operated

The legal requirement from § 109(4)(1), clause 1 of the TKG is regularly satisfied with the creation and submission of a network structure plan. The plan drawn up should describe at least the following structural elements:

1. All telecommunications and data processing systems (switching facilities, service servers, network management) and data processing installations used (customer data management, billing) that are integrated into the network.
2. All connections between the systems (LAN connections, backbone technologies, as well as radio links).
3. All external connections (interfaces) of the systems (type of connection, Internet, remote, roaming).
4. Size and type of network (number of subscribers; mobile, microwave or cable network, etc.).
5. Geographical expansion of the network (local, regional, national or international).

The complexity of the network plan can be simplified by forming groups (e.g. by type, configuration, network, location, framework conditions, applications, services, etc.). In the case of larger networks, separate sub-plans (e.g. for order data processing, accounting systems, backbone networks, etc.) can also be useful.

5.1.2 Description of the publicly available telecommunications services provided

In principle, the content of all the public telecommunications services provided by the company are to be described in accordance with § 109(4)(1), clause 2 of the TKG. To draw up the hazard analysis, it makes sense to abstractly deal not only with content but also the respective group of subscribers. If only services are provided, the telecommunications networks that are used should nevertheless be pointed out.

5.1.3 Classification of criticality

The security concept must indicate which hazards are to be expected, § 109(4)(2) of the TKG. To create this forecast, a risk analysis, which usually consists of a protection requirement, threat and risk analysis, must be carried out. The descriptive findings (5.1.1. and 5.1.2) that have already been determined enable an abstract risk analysis and assignment to specific risk situations (criticalities). The decisive factor in determining criticality is the importance of the telecommunications network or service to be protected. In principle, public telecommunications networks and services can be assigned to the following levels of criticality:

Standard criticality: All public telecommunications networks and services.
Elevated criticality: Public telecommunications networks and services, provided that they are of greater importance for the common good.
Increased criticality: Public telecommunications networks and services, provided that they are of tremendous importance for the common good.

Standard criticality

From a constitutional point of view, the importance of the legal interests to be protected by § 109(1) and (2) of the TKG (telecommunications secrecy, data protection and functionality of the network) must be taken into account for individuals. In this respect, a (lower) standard criticality would have to be based on this importance and ensure that the corresponding principles are observed. Security requirements of this kind are essentially laid down in the main part of the catalogue for security requirements.

Elevated criticality

If the network/service to be protected is used by a larger number of subscribers, the importance of the respective network/service increases. In addition to the importance for individuals, there are also common good interests. These common good interests may become important after a certain number of them. An indication for determining a significant number of subscribers may be based on the Postal and Telecommunications Security Act [Post- und Telekommunikationssicherstellungsgesetz - PTSG]. Among other things, the PTSG serves to ensure the functioning of the community by ensuring the basic supply of telecommunication services. In this context of protection, the scope of the law is linked to the

provision of telecommunications services for more than 100 000 subscribers. The Ordinance for Determining Critical Infrastructures according to the BSI Act (BSI-KritisV) also uses the aforementioned values of the PTSG when determining threshold values. It therefore seems reasonable to presume a particular importance of the network or service within the meaning of § 109(2)(5) of the TKG and to assume a high level of criticality for the telecommunication service offers or the operation of telecommunication networks with a corresponding number of subscribers.

Increased criticality

In addition to the number of subscribers, particularities of the telecommunications network/service to be protected can also indicate a certain importance for the common good or at least further confirm the assumption of a special importance. The public mobile network has a special position in this context. This is because, in the case of the mobile network, cross-sectional use can be assumed in all areas of public life. The availability and security of this network is therefore likely to affect not only individuals, but the state, the economy and society in equal measure.

The operation of 5G networks in accordance with EU Recommendation 2019/534 of 26 March 2019 has an enormously special position. In this sense, 5G networks are the future backbone of our increasingly digitised economies and societies. They will process billions of objects and systems with each other as well as in the critical infrastructures of the energy, water, nutrition, health, finance and insurance, transport and traffic sectors as well as the information technology and telecommunications sectors and support security systems. If publicly accessible 5G mobile networks are operated with a number of subscribers greater than 100 000 subscribers, a tremendous importance of these telecommunications networks can be indicated for the common good.

If a tremendous importance can be derived from the number of subscribers and/or the particularities of the telecommunications network/service to be protected, an increased criticality can be assumed. Only public mobile telecommunications networks of the 5th generation with frequency allocations are currently subject to an increased level of criticality.

5.1.4 Concrete risk analysis

The subsequent, concrete risk analysis – regardless of the earlier abstract assignment to a specific criticality – is to determine and evaluate the components actually operated in each case.

Therefore, all of the company’s security-relevant components must first be identified. Security-relevant components in this sense include all subsystems/systems or business

processes related to telecommunications secrecy, data protection and the availability of telecommunications networks and telecommunications services. Security-related components may also result from organisation. In this respect, the company's security organisation (Section 3.1) must also be subjected to a corresponding risk analysis. In individual cases, the security of data, systems and facilities (Section 3.3) or of the respective company (Section 3.4) is to be forecast. The BSI standards and the components of the BSI IT-Grundschutz Compendium provide further information on these topics, including information on infrastructure, IT systems, networks and applications.
Here, too, the BSI IT-Grundschutz Compendium provides important information on elementary threats from the areas of force majeure, organisational deficiencies, human error, technical failure and intentional actions.

5.1.5 Risk analysis of the overall system

It is not only possible for a dangerous situation to result from isolated operational components or from the abstract allocation of a network. The interaction of various sub-processes can also trigger certain hazards and make additional protective necessary. In this regard, an additional assessment of the overall system is therefore necessary.
Not all sources of danger can always be identified. A corresponding dark field should therefore be taken into account. In a final risk assessment, this existing residual risk must be described and assessed in more detail. However, the aim should be to identify all threats or to reduce them to a quantifiable and acceptable level.

5.1.6 Definition and description of the technical precautions or other protective measures

1. After completing the risk analysis, the obligated company must select and implement suitable, necessary and appropriate protective measures.
An assessment of individual cases is always decisive for selection and determination.

The state of the art must be taken into account when determining the measure. The obligation to take into account the state of the art makes a dynamic adaptation to the changing technical possibilities and risks necessary. In this respect, the assessment of the protective measures is not conclusive but continuous. However, recourse to the state of the art does not include methods that have not yet been used in practice. State-of-the-art measures must be both ready for the market and tried and tested in practice.

The company's interests also play a role in determining measures. The protective measures to be taken in individual cases are only appropriate if the technical and economic effort is appropriately proportionate to the importance of the rights to be protected and the importance of the facilities to be protected for the general public. There must be no disparity between the effort to be made and the benefit to the general public.

In this context, existing protection can be taken into account for newly defined protective measures on a case-by-case basis. Protective measures that were created on the basis of the 'catalogue of security requirements' (version 1.1 of 7/1/2016) can therefore still be considered appropriate in individual cases. However, a prerequisite is that no current changes in the operated public telecommunications networks or the publicly available telecommunications services and thus no change in the risk situation can be determined. A further prerequisite is that the life cycle of the technology used in the networks operated or the services offered must be manageable. The security concept drawn up does not have to be replaced or re-submitted in these cases. In any case, deviations due to inventory protection must be documented and it must be demonstrated that the existing measures are sufficient.

2. Based on the abstract risk analysis, the following principles can apply to the selection of protective measures:

Standard criticality: The technical, organisational, personnel-related and infrastructural measures to be taken must be suitable to ensure a generally recognised level of security. The BSI's IT-Grundschutz offers a selection of concrete recommendations. The components of the IT-Grundschutz Compendium are divided into ten layers and deal with a wide variety of information security topics – from applications (APP) to industrial IT (IND) to security management (ISMS). In individual cases, a higher level of protection may be required to protect telecommunications secrecy.

Elevated criticality: The measures to be taken must be suitable to guarantee a generally recognised level of basic protection as well as increased protection for the areas that are significantly relevant for the elevated level of criticality. In addition, necessary and appropriate measures must be taken against significant disruptions as a result of natural disasters, particularly serious accidents, sabotage, terrorist attacks or other comparable events. Suitable and appropriate measures in this regard must also be provided for in the event of tensions or national defence. This particularly affects emergency preparedness measures. The BSI IT-Grundschutz Compendium offers assistance in selecting specific measures.

Increased criticality: The measures to be taken must be suitable to guarantee generally recognised level of protection, which, in addition to the general need for protection (increased basic protection), also takes into account the special criticality. Operators of public telecommunications networks and providers of publicly accessible telecommunications services that are assigned to this group must also comply with the security requirements and measures specified in Annex 2.

Telecommunications service providers with an IP infrastructure must also take into account the requirements and instructions in Annex 1 ‘Requirements for telecommunications service providers with an IP infrastructure’ when defining protective measures.

However, it is not the abstract assignment to a hazard situation but always the result of the concrete, individual hazard analysis that is decisive for the determination of the protective measures. The assignment of a network or service to a specific criticality may, however, have an indexing effect. In addition, the overall forecast must be taken into account in all cases.

In principle, the obligated company is not obliged to carry out protective measures based on the analysis described above. A determination can also be based on suitable standards and norms (e.g. BSI standards, BSI IT-Grundschutz methodology, DIN ISO/IEC standards).

5.1.7 Drawing up a security concept

After the hazard analysis is completed and the measures to be taken in each individual case are determined, the concept must be drawn up. It must be a cohesive document in terms of content. Only oral communications or declarations made by telephone do not meet these requirements.

5.1.8 Appointment of the security officer

The designation of the security officer is not a direct component of the security concept. However, the designation, like the creation of the concept, must take place when the business or service is started. In this respect, there is both a temporal and contextual relation between these obligations. The security officer should be given certain coordination, control and specialist tasks. The security officer or the designated representative should also be the contact person of the Federal Network Agency.

In accordance with the performance of this task, the agency should maintain the necessary specialist knowledge and an understanding of company processes. The agency's knowledge of developments in IT security, processes in the company and the legal framework must be kept up to date. The prerequisites for direct contact with the company management must be created.

5.1.9 Declaration of implementation

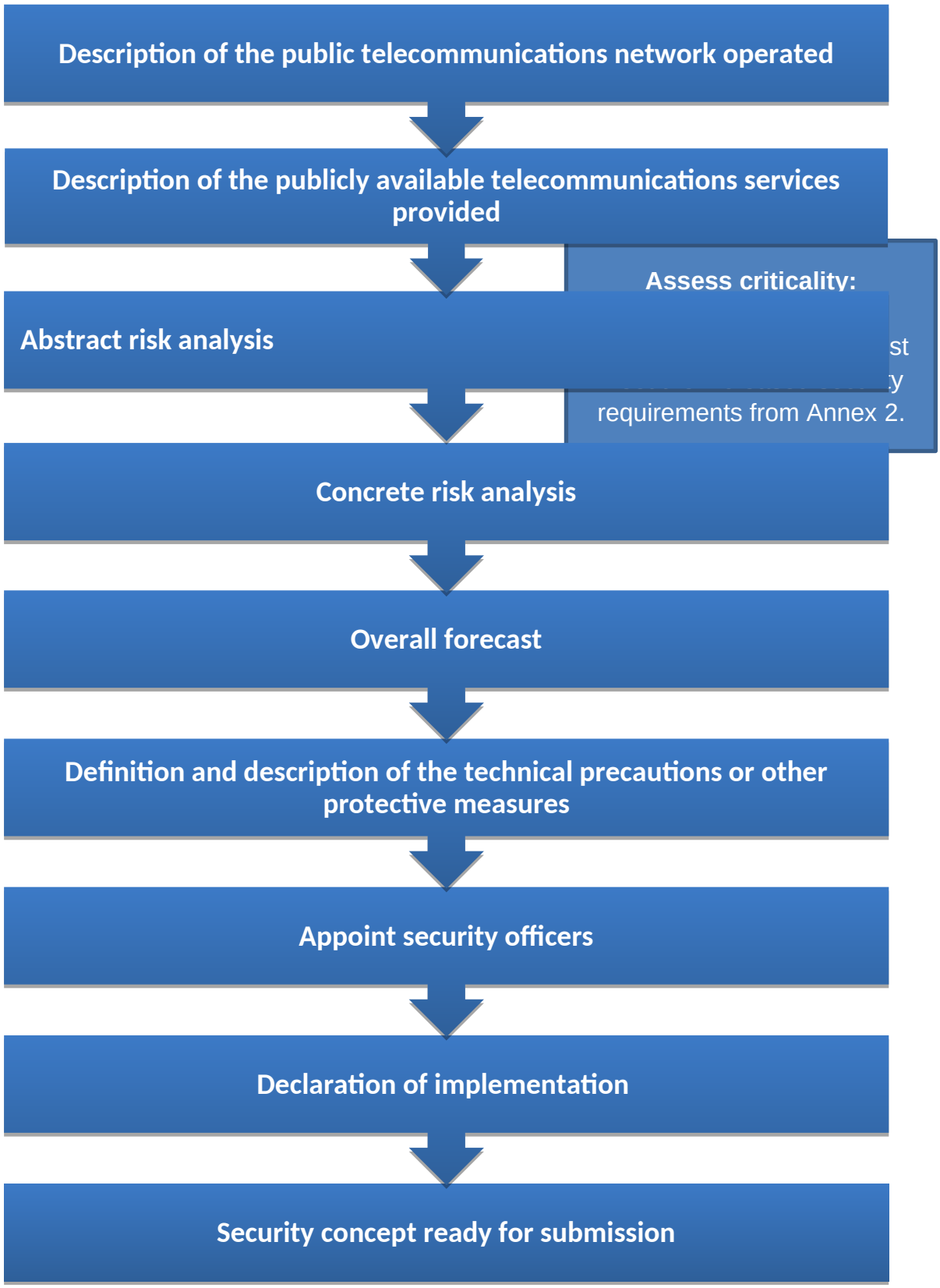
A declaration must be submitted with the security concept stating that the technical measures and other protective measures shown therein have been implemented or will be implemented immediately. The declaration must be in writing.

5.1.10 Adapting the security concept to changes

The security of telecommunications networks and services is a process of continuous improvement. The security concept must therefore be checked regularly and adapted in the event of changes. It must be ensured that technical developments, any weak points that have been identified and any security gaps that have been uncovered are reacted to and that suitable protective measures are taken.

In order to permanently ensure the success of the protective measures in a constantly changing environment (business processes, IT landscapes, laws and regulations, threats, etc.), it must be ensured that the effectiveness of the implemented security measures is determined and assessed at regular intervals. If security problems are identified, improvement measures must be systematically taken, implemented and documented. If the circumstances underlying the security concept change, the obligated party must adapt the concept and submit it to the Federal Network Agency again, with reference to the changes.

5.1.11 Procedure for drawing up the security concept



Beschreibung des betriebenen öffentlichen	Description of the public

Telekommunikationsnetzes	telecommunications network operated
Beschreibung der erbrachten öffentlich zugänglichen Telekommunikationsdienste	Description of the publicly available telecommunications services provided
Abstrakte Gefährdungsanalyse	Abstract risk analysis
Kritikalität bewerten: Infrastrukturen mit erhöhtem Gefährdungspotenzial müssen erhöhte Sicherheitsanforderungen aus Anlage 2 erfüllen.	Assess criticality: Infrastructures with an increased risk potential must meet the increased security requirements from Annex 2.
Konkrete Gefährdungsanalyse	Concrete risk analysis
Gesamtprognose	Overall forecast
Festlegung und Beschreibung der technischen Vorkehrungen oder sonstigen Schutzmaßnahmen	Definition and description of the technical precautions or other protective measures
Sicherheitsbeauftragten benennen	Appointing security officers
Umsetzungserklärung	Declaration of implementation
Sicherheitskonzept zur Vorlage bereit	Security concept ready for submission

6 Entry into force and transitional regulations

The catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data will come into force upon publication in the Official Journal of the Federal Network Agency. The obligated parties must meet the requirements of the catalogue no later than one year after its entry into force, unless the catalogue specifies special transitional provisions.

Sources of information:

ENISA Technical Guideline on Security measures for Article 4 and Article 13a:

https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a

BSI Standard 200-2:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html

BSI IT-Grundschutz Compendium:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

German version EN ISO/IEC 27001:2017

German version EN ISO/IEC 27002:2017

7 Definitions

ENISA
European Agency for Cybersecurity (formerly European Network, Information Security Agency).

Traffic data, § 3(30) TKG
Data that is collected, processed or used when a telecommunications service is provided.

Service provider, § 3(6) TKG
Anyone who wholly or partially provides

- telecommunications services commercially or
- contributes to the provision of such services.

Subscriber, § 3(20) TKG
Any natural or legal person that has concluded a contract with a provider of **publicly accessible** telecommunications services for the provision of such services**.**

Inventory data, § 3(3) TKG
Subscriber data that is collected via telecommunication services for the establishment, content, modification or termination of a contractual relationship.

Telecommunications systems, § 3(23) TKG

Technical facilities or systems that can send, transmit, convey, receive or control identifiable electromagnetic or optical signals.

Telecommunications services, § 3(24) TKG

Services usually provided for a fee that consist entirely or predominantly of the transmission of signals via telecommunications networks, including transmission services in radio networks.

Personal data

Any information relating to an identified or identifiable natural person (hereinafter ‘data subject’); an identifiable person is a natural person who can be identified directly or indirectly, in particular by assigning an identifier such as a name, an identification number, location data, an online identifier or one or more special characteristics that express the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person.

Protective objectives

General protection objectives are the protection of personal data and the protection of telecommunications secrecy. Special protection objectives are the protection of the telecommunications infrastructure from disruptions and risks as well as the availability of telecommunications services.

Annex 1: Requirements for telecommunications service providers with an IP infrastructure

Annex 2: Additional security requirements for public telecommunications networks and services with an increased risk potential

Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data

pursuant to
§ 109 of the Telecommunications Act (TKG)

Version 2.0

Annex 1

Requirements for telecommunications service providers with an IP infrastructure

As at: 29/04/2020

Table of Content

S

1 Introduction

The connection of a telecommunications system to the Internet or the provision of telecommunications services on the Internet harbours a considerable risk potential for the connected telecommunications and IT systems and their users.

An overview of current threats can be found, for example, in the annual situation reports by the BSI[1] and the ENISA[2].

Due to this specific risk situation and due to the importance of the Internet in business and private areas, the telecommunications providers with an IP infrastructure must take suitable security measures. This Annex describes technical and organisational measures for improving Internet security. These measures are to be implemented in accordance with the current state of the art.

Additional recommendations can be found in the series on Internet security (ISi series) and the cybersecurity recommendations for Internet service providers by the BSI.

2 Infrastructure

2.1 Routing and protocols

If various standards or protocol variants are available for the implementation of a service, then, after careful consideration, a solution that can be assessed as the safest according to the state of the art must be implemented.

2.1.1 Encryption technology

The telecommunications provider must encrypt data at security-relevant points according to the state of the art . In particular, state-of-the-art passwords must at least be hashed, salted and stored.

In addition to encrypting the data itself, encryption on the transport route by means of TLS is also an option. The encryption is transparent to users (i.e. without effort on their behalf). Commonly used protocols that support this are HTTPS and SMTPS. The type of encryption and the associated key management must be appropriate to the protection requirements.

[1] BSI situation report (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html)

[2] 'ENISA Threat Landscape Report' (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape)

The respective state of the art must be taken into account here. The BSI's technical guideline TR-02102 offers further assistance.

2.1.2 Protection against DoS/DDoS attacks

In general, the telecommunications provider must take measures to prevent (mitigate) DoS/DDoS attacks. Such mitigation concepts can either be implemented and operated by the Internet operator itself or by a service provider specialised in this.

*2.1.2.1 **Resilience of the infrastructure against DoS/DDoS attacks***

The telecommunications provider's infrastructure must be adequately dimensioned to protect against DDoS attacks. The capacities of systems that could be the focus of DDoS attacks must be designed in such a way that their functionality is guaranteed without further measures even in the case of a moderate attack.

*2.1.2.2 **Protection against IP spoofing***

In order to prevent reflections attacks, for example, telecommunications service providers with an IP infrastructure must take measures that prevent or make it more difficult to forge sender addresses. The requirements from IETF RFCs RFC2827 and RFC3704 must be implemented.

*2.1.2.3 **Deactivation of unused services***

Telecommunications providers should secure their own servers against misuse, for example by deactivating services that are not required. Their customers should be made aware of open ports and accessible services (self-identified or based on external sources) that pose a potential risk to third parties.

*2.1.2.4 **Protection of operationally required services***

Services required for network operation must be protected against DoS/DDoS attacks by suitable measures and components.

One example of a measure is the use of access restrictions or ACLs.

The components can be packet filters or DDoS mitigation devices, for example.

*2.1.2.5 **Detection of botnets***

Telecommunications service providers with an IP infrastructure must operate a suitable sensor system in order to detect botnets, taking into account the provisions in § 100(1) of the TKG. In individual cases, connection to existing connections is also permitted in order to detect and limit faults in accordance with § 100(2) of the TKG. However, this may only occur if there is an operational need and milder means, such as an evaluation of traffic or control data of an information technology protocol, do not contribute to achieving the objective. Protection requirements under data protection law, such as the immediate deletion of recorded data and the notification of the company data protection officer, must be observed, see § 100(2) of the TKG.

2.1.3 Principle of equal treatment

The telecommunications provider must transmit data packets to and from customers without changes and equally, regardless of where they come from or which applications generated the packets. An exception to this is the telecommunications provider's VOIP service, which can be operated via separate networks and/or with a reserved bandwidth.

2.1.4 Inter-domain routing

Measures must be taken to prevent the manipulation of BGP routes. The use of RPKI, for example, lends itself for this.

2.2 Monitoring, reporting and cooperation

In order to detect attacks or faults, the traffic data should be regularly monitored for any abnormalities within the scope of the legal possibilities and insofar as this is necessary for the provision of the respective service. If irregularities are found, suitable protective measures must be taken (e.g. stopping network traffic, restricting or stopping traffic to interferers). In particular, the GDPR and § 100(1) of the TKG must be observed here and § 109a(4) to (6) of the TKG must be observed for the measures. Here, the recommendation in the guidelines from the BfDI and the BNetzA for a data protection-compliant storage of traffic data[3], which is to erase the data after seven days at the latest if no there are no specific indications of attacks or faults, should be followed.

In individual cases, the telecommunications content can also be recorded to identify and limit faults under the conditions as per § 100(2) of the TKG (see 2.1.2.5).

Furthermore, the measures described in this Annex should be implemented in order to be able to detect or exclude undesired changes by manufacturers, management service providers or state actors (e.g. from the manufacturing countries).

2.2.1 Implementation of a monitoring infrastructure

2.2.1.1 ***Scope***

A suitable monitoring infrastructure (MI) must be provided. It should be able to continuously identify and prevent threats. A suitable MI must also provide for appropriate remedial measures to be taken in the event of malfunctions. It should be possible to implement the measures envisaged effectively and, if necessary, under time pressure.

The MI must record all components essential to the operation of the network as well as components that transmit personal data (e.g. user IDs) to external contractual partners, for example in the context of cross-network signalling. Suitable data sources for security monitoring may include BGP routers, servers for DNS, email, HTTP(S), SIP(S), SSH, IPsec.

Significant deviations from normal network operation (e.g. unusual data flows, atypical data packets at certain ports, conspicuous behaviour of critical network components etc.) must be permanently registered, analysed and documented. It is important to ensure that the data is only stored for the required period of time. If there are no concrete indications of attacks or

[3] See point B.I.2 in the guideline dated 19/12/2012.

faults, the data must be anonymised (e.g. by preparing statistical evaluations) or erased after seven days at the latest.

2.2.1.2 ***Tools and documentation***

The tools used for monitoring must continuously and automatically record and evaluate suitable parameters or features from ongoing operations. The working method, the interaction of the monitoring tools and any data processing that may have been carried out should be documented in the security concept. Threshold values and similar parameters that are used to adjust the MI (e.g. frequency of individual events until an alarm is triggered, adjustment of the ratio of true positives to false negatives) should also be documented.

The method for dealing with identified abnormalities must also be documented. The measures that are automatically initiated by the MI and that trigger an alarm that entails manual intervention must be indicated.

In addition, the MI should generate statistics that are independent of the individual case and enable identification of a specific hazard or modus operandi. If binary classifiers are used, they should be evaluated by looking at the key data together (TPR, FPR, TNR, FNR) and by means of suitable representation (e.g. ROC curve).

2.2.1.3 ***Further development***

The data generated by the MI should be reviewed on a regular basis to optimise the relationship between true positives and false negatives. External data sources should also be used to identify false negatives. In these cases, too, the measures taken for optimisation (e.g. adjustment of threshold values; the acquisition of additional parameters; the use of additional monitoring tools or the deactivation of monitoring tools that are no longer appropriate) and any changes to the MI should be documented.

An MI must be legally permissible and compliant with data protection. From the point of view of telecommunications law, the legal admissibility of an MI is based on § 100(1) and (2) of the TKG.

2.2.2 Recording/logging of management activities

All management activities on network components must be logged and archived for a sufficiently long period of time depending on their importance to the security of the overall infrastructure so that possible security incidents can also be subsequently reconstructed.

2.2.3 Logging the configuration files

The target configuration of each network component should be documented and stored such that it is protected against unauthorised access.

2.2.4 Target/actual comparison of the components

Revisions of the network infrastructure should be carried out sufficiently frequently and include a target-actual comparison of the current configuration files of all network components with the reference files archived in accordance with 2.2.3.

2.2.5 Behavioural testing of the components

In addition to the target/actual comparison of the configuration files, the actual and intended behaviour of individual components should be regularly compared. For this purpose, test cases are to be defined in which the compliant behaviour is described.

2.2.6 Identifying infected systems and educating the customer about threats when an infection is detected

In addition to the aforementioned precautions for their own protection, telecommunications providers should also monitor the network with regard to infected customer systems. The measures required for this are to be designed according to the state of the art and taking into account the legal requirements. If the telecommunications provider becomes aware of faults that originate from the user's data processing systems, it is obliged under TKG § 109a(4) to notify the users immediately, insofar as this is technically possible and reasonable. In this case, it must also point out to the users appropriate, effective and accessible technical means with which they can identify and remedy these faults. The legal reporting obligations (see catalogue Chapter 3.5.3) must be observed.

2.2.7 Cooperation in the event of faults affecting multiple telecommunications providers

If faults occur that could affect several telecommunications providers, for example due to DDoS attacks (see also 2.1.2.), cooperation between telecommunications providers is necessary. This should also include a cross-provider exchange regarding infected devices.

For this purpose, contacts and procedures must be coordinated with one another in advance. This also includes naming an abuse contact that is responsive at least during office working hours and processes incoming reports (possibly automatically).

It is the telecommunications provider's responsibility to contact networked providers in order to identify the appropriate contact persons. In return, the latter must immediately inform the first telecommunications provider of any changes. It must always be ensured that direct and immediate contact between telecommunications providers is possible in an emergency.

2.2.8 Cooperation with anti-malware manufacturers

The immediate forwarding of malware samples to AV manufacturers should assist them in the timely improvement of detection measures.

3 End user services

3.1 General safety precautions

In addition to authentication with the help of a user name and password, if technically possible, customers should be offered stronger authentication methods such as cryptographic authentication methods or two-factor authentication methods (possession and knowledge).

3.2 Internet access

3.2.1 New customer information

New customers should be provided with information in writing about risks on the Internet, existing protection options and information on how to remove malware.

3.2.2 Informing the customer if a malware infection is suspected

If it is suspected that a customer's device is infected with malware, the customer should be notified.

3.3 VoIP

3.3.1 Bandwidth, availability of emergency numbers

The telecommunications provider should reserve part of the available bandwidth for VOIP communication. Above all, the availability of emergency numbers must be ensured.

3.3.2 Confidentiality of communication

In addition to Section 2.1.1, VoIP data should, within the realm of what is technically possible and economically feasible, be transferred in an encrypted manner both in the case of transfer between provider networks and – if the customer's CPE offers the technical prerequisites for this – between the customer CPE and the provider's SBC.

3.3.3 Transmission of phone numbers

The signalling for CLIP/CLIR must be set correctly for outgoing connections and correctly taken into account for incoming connections. Furthermore, the network provided number and the user provided number must be transmitted correctly.

3.3.4 Protection against TDOS

To the extent that this is technically possible and economically appropriate, telecommunications providers should be able to recognise and prevent automated mass calls to a connection for the purpose of paralysing it (TDOS attacks), for example through appropriate monitoring on the SBC.

3.4 DNS services

3.4.1 Protection against spoofing and aggravation reflection/amplification attacks

To protect against spoofed DNS requests, telecommunications providers must ensure that DNS resolvers, insofar as they are under their own operational responsibility, are not openly accessible ('open resolver'), but that accessibility is restricted to their own customer base. Permanent monitoring of the DNS server must be guaranteed and should make it possible to

detect reflection/amplification attacks at an early stage. Indications arise, for example, when requests from certain sources accumulate, with regard to certain resource records, unauthorised recursive requests, etc. In these cases, countermeasures such as restricting and filtering requests must be taken. This also applies to services such as NTP, SSDP, etc., which are also increasingly being abused for reflection attacks.

3.4.2 Protection against DNS cache poisoning

To increase the server's robustness against DNS cache poisoning attacks, port randomisation should be activated. The traffic volume should be monitored regularly in order to detect cache poisoning attacks at an early stage. Especially in the case of broadband connected DNS resolvers, a cache poisoning attack is still possible despite activated port randomisation. To reduce risks, upper limits should also be set for the holding period of buffered data in the DNS cache.

3.4.3 Use of DNSSEC

DNSSEC signatures must be validated across the board within the network operator's DNS infrastructure. The telecommunications provider should educate its customers about the advantages of DNSSEC and encourage them to make use of them.

4 Acronyms

RFC document describing Internet standards

TPR True Positive Rate

FPR False Positive Rate

TNR True Negative Rate

FNR False Negative Rate

ROC Receiver Operating Characteristic

Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data

pursuant to
§ 109 of the Telecommunications Act (TKG)

Version 2.0

Annex 2

Additional security requirements for public telecommunications networks and services with an increased risk potential

As at: 13/05/2020

Table of contents

1 Field of application

Additional security requirements for networks and services with increased criticality are described below. The sequence of the additional safety requirements described is based on the life cycle (production, delivery and commissioning) of the components to be assessed.

2 Certification of critical components

2.1 Basic principles

The responsible national authority for the IT security certification of critical components is the Federal Office for Information Security (BSI). The BSI is also responsible for the national recognition of test centres as part of the national IT security certification.

In consultation with the Federal Network Agency, the BSI will draw up and publish a technical guideline for the networks concerned within the scope of this Annex. It contains requirements for the certification of critical components, including requirements for the application environment and for operation as a prerequisite for the validity of certificates. In addition, it describes conditions for the provision of certificates according to European certification schemes (CSA). The following sections describe the process for identifying the critical components and regulations on their use, based on the list (see below) of the critical functions in a telecommunications network.

2.2 List of critical functions

Together with the BSI, the Federal Network Agency will create a document that lists the critical functions in a telecommunications network.

Critical functions are identified by BNetzA and BSI on the basis of a joint risk analysis and on the basis of the current state of the art and are included in the list.

According to the BNetzA and BSI's assessment, the list is continuously updated, especially if essential conditions have changed. The results of national or international risk analyses such as ENISA or BEREC are taken into account.

The BfDI is given the opportunity to participate in drawing up and updating of the list.

Manufacturers, associations of public telecommunications network operators and associations of providers of publicly available telecommunications services are given the opportunity to comment. The list will be published in the Official Journal of the Federal Network Agency.

2.3 Identification of critical components

Components that realise critical functions in part or in full must be identified and documented as critical components. The network operator will indicate the planned installation of the critical component to the BSI and BNetzA.

Transitional regulation: This requirement must be implemented at the latest one year after the list of critical functions has been published.

2.4 Certification of critical components

I) Components for the realisation of critical functions may only be used if they have been checked in terms of IT security by a recognised testing body and certified by a recognised certification body in accordance with Regulation (EU) 2019/881 (Cybersecurity Act).

If no corresponding certification schemes are available, obligated network operators and service providers must temporarily take other suitable and appropriate technical precautions and other hazard prevention measures when using critical components.

As part of product certification, requirements are often placed on the operating environment or the safe operation of products. Safe operation can only be guaranteed if the requirements described in the certificate or by the manufacturer are met.

Details on the requirements from 2.4, in particular on the certification schemes to be used, are regulated in the BSI's Technical Guideline.

II) Regulations:

The following regulations apply with regard to the requirements for the use of certified critical components:

<u>Commissioning of components after 31 December 2025</u>

For critical components that are put into operation after 31 December 2025, the requirements for the use of certified critical components in accordance with 2.4(I) apply.

Commissioning of components by 31 December 2025

Critical components that are or have been put into operation by the end of 31 December 2025 should meet the requirements from 2.4 (I) from the point at which two suitable, appropriately certified products from different manufacturers are available on the market, but no later than 31 December 2025. If non-certified products are used from this point in time until 31 December 2025, the obligated party must justify this as well as demonstrate and document that no additional hazards are to be expected as a result and that the obligated party will therefore not be subjected to any relevant security breaches in accordance with § 109(5) of the TKG. Subsequent certification is not required for existing components that are no longer newly installed. If a critical component already used on the network does not obtain certification or loses it, the component must be replaced on the network by 2025. This also applies to existing components.

The Federal Network Agency takes measures and implements other orders under the TKG to ensure compliance with these requirements.

3 Trustworthiness of manufacturers and suppliers

The certification of a critical component or functionality is not directly linked to the trustworthiness of the respective supply source (supplier). However, the use of critical components from unknown or untrustworthy sources can open up considerable sources of danger. For use in a sensitive environment, the supply source of the critical component is therefore essential in addition to its certification.

A critical component can be obtained from a manufacturer (§ 434(1), sentence 2 BGB) or a seller or supplier (§ 445a(1), sentence 1 BGB). Against this background, public telecommunications network operators and providers of publicly accessible telecommunications services with increased criticality are required to, in particular, appropriately select manufacturers and sellers or suppliers of critical components before purchasing them. An appropriate selection also includes an appropriate examination of the

supply source's trustworthiness. The obligated company must obtain a comprehensive declaration from the supply source to demonstrate its trustworthiness. The declaration must relate to all safety-relevant components and, if applicable, functionalities, as well as the supply source itself (the manufacturer, including the supplier, and, if applicable, the seller or supplier).

A non-exhaustive list of the content of a declaration of the trustworthiness of a supply source is provided below. Breaches of the declaration should be punished with contractual penalties. The specific content is to be determined by the obligated company in each individual case.

1. Obligation of the supply source to cooperate intensively with the consumer in the field of security technology and, in particular, to provide information at an early stage about new products, technologies and updates of existing product lines.

2. Assurance from the supply source that no information from its contractual relationships with the consumer or one of its offices will be passed on to third parties.

3. Obligation of the supply source to ensure, through organisational and legal measures, that confidential information from or about its customer(s) does not end up abroad at its own initiative or at the initiative of third parties or that foreign agencies in Germany become aware of it.

4. Assurance from the supply source that it is legally and actually able to refuse to disclose confidential information from or about its customers to third parties. In particular, at the time the declaration is made, there are no obligations to disclose such information to third parties or to make it available in any other way. This does not apply insofar as there are statutory disclosure requirements for law enforcement purposes, unless such disclosure obligations exist towards foreign intelligence or security authorities. In cases of doubt, the supply source must refer to the statutory disclosure obligation(s) before the declaration is submitted.

5. Obligation of the supply source to notify the user immediately in writing if compliance with the declared obligation can no longer be guaranteed, in particular if a need or obligation arises for it or if it could have recognised one that could prevent him from fulfilling this obligation.

6. Obligation of the supply source to provide specific information about the product development of the safety-related system parts of its products on request.

7. Obligation of the supply source to use only particularly trustworthy employees for the development and manufacture of the safety-critical system components.

8. Declaration of willingness of the supply source to agree to security checks and penetration analyses on its product to the required extent and to provide appropriate support.

9. Assurance from the supply source that the product for which the declaration is made does not have any deliberately implemented vulnerabilities and that these will not be installed at a later date and that all known unintended vulnerabilities have been remedied or will be remedied immediately in the future.

10. Obligation of the supply source to immediately report known weaknesses or manipulations or ones that become known to the consumer so that measures can be taken at an early stage to limit and remedy possible consequences of quality defects. If the manufacturer obtains information that impairs the safety and functioning of its products or that may negatively influence intended operation, this will be communicated to the consumer immediately. The manufacturer also undertakes to provide solutions immediately.

11. Explanation of whether and how the supply source can sufficiently ensure that the critical component does not have any technical properties that are capable of exerting an abusive influence on the security, integrity, availability or functionality of the critical infrastructure (e.g. through sabotage, espionage)

The measures and requirements described in the following chapters can only be implemented or met in combination with the assurance of trustworthiness.

The explanations apply mutatis mutandis to declarations from the suppliers.

The appropriate selection of manufacturers and suppliers is continued by appropriately monitoring them. If the obligated company becomes aware of indications of a disregard of

the manufacturers' or suppliers' self-declaration, an immediate clarification of the facts must be arranged for and, if necessary, suitable measures to avert danger must be taken. Disregarding the manufacturers' or suppliers' self-declaration may lead to considerable security violations. Please refer to the obligation to report actual or possible significant security breaches (§ 109(5) TKG).

4 Product integrity

A product is exposed to different risks in the respective phases of its life cycle. In order to minimise these risks, requirements are placed on the operator, but also on the functional scope of the components, for particularly critical phases.

4.1 General

The operator must be able to verify the integrity of the purchased components at any time, starting with the acceptance. The test options must be used and documented by the operator.

To ensure that this is possible for the operator, technical methods/procedures must be integrated into the product, and the approach for carrying out the verification must be suitably documented.

Hazardous areas throughout delivery and until commissioning must be explicitly and separately documented in the safety concept by the operator with the manufacturer's support. The following areas are considered particularly dangerous.

4.2 Delivery

A delivery starts when the components leave the manufacturer's area of control. Delivery ends with acceptance by the operator. The delivered components must be protected against possible manipulation or other influences in this hazardous area. This can be ensured by means of product-internal or external mechanisms. Certain basic methods/procedures are currently available to ensure this.

A suitable measure for software products is the use of cryptographic procedures to ensure integrity. Suitable physical protection must be provided for hardware products, such as

sealed transport boxes, guarded transport or self-protection of the product (possible, for example, for SIM cards). The exact design of these mechanisms can, in principle, be manufacturer-specific.

4.3 Acceptance

An acceptance in the sense of this Annex 2 is when a component is ready for operation and free of defects after inspection by the receiving operator and the operator expressly declares acceptance.

In particular, the operator must check whether the components in question have been tampered with, interfered with or modified in the course of delivery. Suitable checks are generally available for this within the framework of the procedures already mentioned.

4.4 Storage

Storage refers to the part of the supply chain between acceptance and commissioning. The operator must also ensure the integrity of the components in this hazardous area. This can also be ensured by means of internal and/or external mechanisms. Before possible storage, a functional test and a check of the integrity of the components must be carried out at least on a random basis.

4.5 Commissioning

Commissioning takes place when the components are transferred to the operations of the network. The operator must once again perform an integrity check and include this in the configuration management. Suitable checks are also available for this purpose within the framework of the mechanisms already mentioned.

4.6 Live operation

See Chapter 5 Safety requirements during operation.

4.7 Decommissioning

Special requirements (e.g. secure deletion of key material, configurations, personal data such as traffic data, etc.) may also have to be taken into account for decommissioning. For this purpose, appropriate technical methods/procedures must be integrated into the product, and the approach for carrying out the decommissioning must be suitably documented for the operator.

5 Safety requirements during operation

Safe commissioning does not guarantee the permanently safe operation of the public telecommunications network. Rather, new, different sources of danger arise during operation. In order to ensure that § 109(1) to (3) of the TKG is continuously ensured, the obligated company must also take technical measures and other measures that are suitable and appropriate to the potential risks. In this sense, the use of monitoring procedures is suitable.

5.1 Security monitoring

The obligated company must implement and operate a monitoring infrastructure (MI) in order to continuously identify, limit or remedy faults or errors in telecommunications systems. In addition to the requirements in paragraph 2.2 of the ‘Annex: Requirements for Telecommunications Providers with an IP Infrastructure’ the following requirements apply:

The MI must record all critical components as well as components that transmit personal data (e.g. IMSIs, CDRs, MSISDN, IMEIs) to external contractual partners, for example in the context of cross-network signalling or roaming. Suitable data sources for security monitoring include servers for SS7, DEA, SEPP, NRTRDE and infrastructure components such as SMSC or HLR.

Faults or errors in telecommunications systems can result, for example, from DoS and DDoS attacks; botnets; unwanted and missed calls (‘Wangiri’); PBX hacking; incoming mass calls or SMSs to one or more subscribers (robocalling, SPIT); outgoing mass calls or SMSs, potential call ID forgery; anomalies in the context of the applications offered (e.g. from the area of M2M communication or IoT).

Threats also arise from false base stations. These should therefore be recognised by a suitable MI without the involvement of the users' end devices (hardware or software).

5.2 Cryptographic mechanisms and key management

The obligated company must describe its key management in its security concept. The life cycle of cryptographic keys and the technical and organisational measures taken to protect these keys must be documented. For example, the documentation must comprise key material

- in the UICC or eUICC as well as copies in the infrastructure,
- for the encryption of the SUPI,
- for operation in the context of remote SIM provisioning,
- for the operation of the N32 interface and DIAMETER,
- for the operation of the SIP infrastructure
- to secure communication between network components, and
- to secure communication between network components and the central network management

. The purpose of this list is to provide orientation and does not claim to be exhaustive.

If keys are generated by the provider, the process used for the generation must be documented. If confidential keys or certificates with public keys are transmitted to the contractual partner, the technical and organisational protective measures used must be documented.

The provider must document which cryptographic algorithms are supported for protecting confidentiality and integrity on the air interface, taking into account the activated configuration. If possible, a distinction should be made between access stratum and non-access stratum, between signalling and user data, and between different network generations (2G/3G/4G/5G etc.). If there are differences that depend on the geographical region, they should also be documented.

6 Instructed specialist staff

The specialist staff employed must have the required professional qualifications to perform the task. This already applies as a basic rule. When dealing with critical components and functionalities, however, particular attention must be paid to determining an appropriate level of competence. In order to properly carry out a safety-relevant task with the existing risk potential, mere knowledge of technical processes is not sufficient. Rather, what is required and appropriate is the additional minimum knowledge of the most common threat scenarios for telecommunications secrecy, data protection and the network's functionality.

Both the state of the art and the corresponding hazard situations are subject to dynamic development. The obligated company should therefore not only statically take care to appropriately select staff, but also constantly monitor the suitability of specialist staff. The content of the training measures to be carried out must at least be based on the state of the art and deal with the development of possible and known hazard situations.

All employees deployed in security-relevant areas should therefore be made aware of their responsibility as part of regular awareness-raising and training measures.

Training and awareness-raising measures must be documented in a suitable form.

It must be ensured that responsibilities and powers are clear and transparent to everyone. A suitable and accessible description of organisation and tasks can establish this transparency.

Particular attention must also be paid to the personal suitability of the staff employed. This is because performing a safety-relevant task requires appropriate behaviour, especially in exceptional situations. The staff employed should therefore be resilient so that tasks and decision-making are ensured in stressful situations. Participation in regular emergency or crisis exercises may be helpful in this context.

The staff employed must be trustworthy. The minimum requirement will therefore be that the identity of the staff in question is established prior to deployment in security-relevant areas. A coherent, substantiated and verified curriculum vitae can establish certainty about the origin of the staff employed.

If staff are deployed in particularly security-relevant areas, it may be appropriate to request the presentation of a certificate of good conduct from the police.

Violations of the rules and inaccurate information provided by the security staff employed must be linked to an appropriate and known sanction under labour law. Rule violations with criminal relevance are to be reported consistently.

7 Redundancies

There are serious consequences if critical components are technically compromised. Appropriate technical precautions or other measures must therefore be taken to protect against faults and to manage the risks. One possible suitable technical precaution is precautionary measures with sufficient redundancies. This is especially true when critical components have to meet very high availability requirements. One goal must be to avoid accidents as much as possible or at least to minimise downtimes. If tampering is identified, provision may be made to provide a fallback option by providing sufficient redundancies.

A suitable risk analysis should, if possible, determine whether and to what extent responsibility can be taken for a failure of critical components without endangering the legal protection objectives. In addition, a check must be carried out to determine whether suitable technical alternatives are available for a failure. For example, the determination and definition of temporary alternative network routes or base stations could be helpful. The security concept should, if possible, specify and describe which network and system components can be activated by operational replacement components or immediately (automatically) in the event of a fault (hot standby). The components for which short-term availability is sufficient thanks to appropriate storage in a warehouse or agreements with suppliers should also be determined and described. It should be noted that certain properties of modern networks and certain application scenarios require high network availability. Ultra-reliable and low-latency communications (URLLC), for example, are very time-critical applications with low latency. Failure should therefore be excluded as far as possible. The security concept should provide for application scenarios tailored to each individual case.

Air conditioning units are an example of possible redundancies. Appropriate monitoring should be carried out in server cabinets and multifunctional enclosures. Irregularities should trigger pre-determined preventive measures. The provision of redundant (e.g. mobile) air conditioning systems may be suitable for avoiding faults.

8 Diversity

When planning and setting up networks, ‘monocultures’ should be avoided by using critical network and system components from different manufacturers. For this reason, components or systems from at least two different manufacturers must be used for the core network (backbone and core network), the transport network and for access networks (radio access networks/wired access networks), unless the MNO’s own developments are used. These should be independent of each other and not equally dependent on a third party. In particular, critical network functions and network elements should not depend on a single provider of critical components based on the network topology implemented. Networks are to be designed topologically in such a way that there is diversity even in the case critical network functions and network elements that are particularly worth protecting. This could be supported by the application of open standards, such as Open RAN, in the event of future developments in the state of the art.

Measures are to be developed that compensate for the short-term non-availability of components of a manufacturer in order to maintain the functionality of the network.