

TITLE

The report title page is designed by the Press Unit and inserted into the file.

Contact person:

Graphic team of the press office: grafik@bnetza.de

(back of front page)

Catalogue of safety requirements

for the operation of

Telecommunications and

Data processing systems

and for processing

personal data according to

Section 167 of the Telecommunications Act (TKG)

State of play: September 2026

(back of front page)

**Federal Network Agency for Electricity, Gas,
Telecommunications, postal services and railways**

Unit 217

Tulip field 4

53113 Bonn

Telephone: +49 228 14-0

Fax: +49 228 14-8872

E-Mail: info@bnetza.de

contents

Inhaltsverzeichnis.....	7
I ENTWURF DES KATALOGS VON SICHERHEITSANFORDERUNGEN GEMÄSS §167 TKG.....	11
A Allgemeinverfügung.....	12
Gründe:.....	15
1. Ermächtigungsgrundlage und formelle Rechtmäßigkeit (Ziffern 1) bis 3) des Tenors).....	15
2. Materielle Rechtmäßigkeit (Ziffer 1) des Tenors).....	16
2.1 Umfang der Regelungswirkung (§ 35 S. 1 VwVfG) sowie Bestimmtheit (§ 37 Abs. 1 VwVfG).....	17
2.2 Unbestimmte Rechtsbegriffe.....	19
2.3 Ermessensausübung.....	20
2.3.1 Entschließungsermessen.....	20
2.3.2 Auswahlermessen.....	20
2.3.3 Kein Ermessens Fehlgebrauch: Allgemeine Verhältnismäßigkeitsüberlegungen hinsichtlich aller im Katalog genannten Maßnahmen.....	21
2.3.4 Widerruf des Sicherheitskataloges Version 2.0 (Ziffer 2) des Tenors).....	26
2.3.5 Gesonderte Rechtmäßigkeitserwägungen zu den Gefährdungspotenzialen (Ziffer 3) des Tenors).....	26
B Katalog von Sicherheitsanforderungen §167 TKG.....	30
1. Einleitung/Allgemeines.....	31
2. Adressaten.....	33
3. Bestimmung von Gefährdungspotenzialen.....	34
3.1 Gefährdungspotenziale.....	34
3.2 Verhältnismäßigkeitserwägungen zur Bestimmung der Gefährdungspotenziale. .	36
4. Festlegung grundlegender Einzelheiten der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Berücksichtigung der verschiedenen Gefährdungspotenziale, § 167 Abs. 1 S. 1 Nr. 1 TKG.....	39
4.1 Schutz des Fernmeldegeheimnisses und personenbezogener Daten.....	41
4.2 Unternehmensführung und Risikomanagement.....	42
4.2.1 Informationssicherheitspolitik.....	43
4.2.2 Risikomanagement.....	43
4.2.3 Sicherheitsrollen und Verantwortlichkeiten.....	44
4.2.4 Sicherheit bei Abhängigkeiten von Dritten.....	45
4.3 Sicherheit im Personalmanagement.....	47
4.3.1 Personalmanagement.....	48
4.3.2 Sicherheitswissen, Sicherheitsausbildung und Prüfung.....	48
4.3.3 Personelle Veränderungen.....	49
4.3.4 Umgang mit Verstößen.....	50
4.4 Sicherheit von Daten, Systemen und Einrichtungen.....	51
4.4.1 Physische und umgebungsbezogene Sicherheit.....	53
4.4.2 Sicherheit der Versorgung (Verfügbarkeit des Gesamtsystems).....	54
4.4.3 Zugriffs- und Zugangskontrolle zu Netz- und Informationssystemen.....	55
4.4.4 Integrität und Verfügbarkeit von Netz- und Informationssystemen.....	56
4.4.5 Sicherstellung der Vertraulichkeit.....	57
4.4.6 Schutz von sicherheitsrelevanten Daten.....	58
4.5 Betriebsführung.....	59
4.5.1 Betriebsverfahren.....	60
4.5.2 Änderungsmanagement.....	60

4.5.3	Asset Management.....	61
4.6	Lifecycle-Management für Hard- und Software.....	63
4.7	Management von Zwischenfällen.....	65
4.7.1	Verfahren für das Management von Zwischenfällen.....	66
4.7.2	Fähigkeit zur Erkennung von Zwischenfällen.....	67
4.7.3	Meldung von Zwischenfällen und Kommunikation.....	67
4.7.4	Kooperation bei TK-anbieterübergreifenden Störungen.....	68
4.8	Notfall- und Ausfallmanagement.....	70
4.8.1	Strategie zur Aufrechterhaltung der Netze, der Dienste und Notfallpläne.....	71
4.8.2	Wiederanlauf nach Ausfällen (Disaster Recovery Management).....	72
4.8.3	Backup-Strategie.....	73
4.9	Überwachungs-, Prüf- und Testverfahren.....	74
4.9.1	Systeme zur Angriffserkennung, Überwachungs- und Protokollierungsmaßnahmen.....	75
4.9.2	Notfallübungen.....	76
4.9.3	Testen von Netz- und Informationssystemen.....	76
4.9.4	Beurteilung der Schutzmaßnahmen.....	77
4.9.5	Überwachung der Einhaltung.....	78
4.10	Bewusstsein für Bedrohungen (Threat Awareness).....	79
4.10.1	Informationen über Bedrohungen (Threat Intelligence).....	80
4.10.2	Information der Nutzer über Bedrohungen.....	80
5.	Festlegung von zusätzlichen Einzelheiten und Maßnahmen für 5G-Netze.....	81
5.1	Bestimmung von kritischen Komponenten.....	81
5.2	Zertifizierung von kritischen Komponenten.....	82
5.2.1	Übergangsregelung zur Zertifizierung von kritischen Komponenten.....	82
5.3	Diversität.....	83
5.4	Technische Maßnahmen für die Sicherheit in 5G-Netzen.....	84
5.4.1	Schutz der Identität und Privatheit der Teilnehmer.....	84
5.4.2	Schutz der Vertraulichkeit der Nutz- und Signalisierungsdaten.....	88
5.4.3	Schutz der Integrität der Nutz- und Signalisierungsdaten.....	89
5.4.4	Schutz des Zugriffs auf Netzwerkfunktionen im 5G-Kernnetz.....	91
5.4.5	Schutz der SBA-Kommunikation im 5G-Kernnetz.....	92
5.4.6	Schutz der Kommunikation zwischen Zugangsnetzwerk und Kernnetz sowie zwischen Zugangsnetzwerken.....	93
5.4.7	Schutz der Kommunikation innerhalb eines Zugangsnetzwerks.....	95
5.4.8	Schutz der Kommunikation zwischen dem 5G-Kernnetz und Nicht-5G- Netzwerkelementen.....	96
5.4.9	Schutz der Roaming Signalisierung.....	98
5.4.10	Schutz des Remote SIM Provisionings.....	100
5.4.11	Schutz vor Angriffen auf die Ausführungsumgebung bei Virtualisierung und Containerisierung.....	101
5.4.12	Schutz bei Nutzung von Virtualisierungs- oder Cloud-Diensten.....	103
6.	Empfehlungen und Hinweise.....	105
6.1	Lokales Breitband 26 GHz.....	105
6.2	Zugrundeliegende Normen, Standards und Guidelines.....	105
	Glossar.....	106
	Abkürzungsverzeichnis.....	107

C Anhang 1 - Technische Spezifikation für paketvermittelte Netze zum Katalog der Sicherheitsanforderungen.....109

1.	Einleitung.....	109
2.	Maßnahmen gegen Distributed Denial of Service (DDoS) Angriffe.....	111
2.1	Ertüchtigung der eigenen Infrastruktur.....	111
2.2	Mitigation.....	111
2.3	Absicherung ausnutzbarer Systeme.....	111
3.	Inter-Domain-Routing.....	113

3.1	Schutz der BGP-Session.....	113
3.2	Bereitstellung von Routing-Informationen.....	113
3.3	Verhinderung der Weitergabe falscher Routing-Informationen.....	113
3.4	Verhindern von Datenverkehr mit gefälschten Quell-IP-Adressen.....	114
3.5	Bereitstellung aktueller Kontaktinformationen.....	114
4.	Domain Name System - Resolver.....	116
4.1	Technische Voraussetzungen.....	116
4.2	DNSSEC.....	116
4.3	Cache-Poisoning.....	117
4.4	Privacy.....	117
5.	Domain Name System - Autoritative DNS-Server.....	119
5.1	Technische Voraussetzungen.....	119
5.2	Schutz vor Ausnutzung.....	119
5.3	DNSSEC.....	120
6.	E-Mail-Sicherheit.....	121
7.	Bewusstsein für Bedrohungen (Awareness).....	122
7.1	Etablieren eines Schwachstellen-Managements.....	122
7.1.1	Systematisches Sammeln und Auswerten der Schwachstellenmeldungen von Herstellern und CERTs.....	122
7.1.2	Informationsaustausch und Zusammenarbeit mit anderen Anbietern und Betreibern.....	123
	Begriffsbestimmungen für Anhang (Technische Spezifikation).....	124
	Abkürzungsverzeichnis.....	126
D	Anhang 2 - Liste der kritischen Funktionen.....	129
1.	Liste der kritischen Funktionen.....	129
2.	Prozess zur Identifizierung von kritischen Komponenten im betriebenen Netz...134	
3.	Verhältnismäßigkeitserwägungen zur Liste der kritischen Funktionen.....135	
II	KONSULTATION.....	137
	VERZEICHNISSE.....	143
	Abbildungsverzeichnis.....	144
	Impressum.....	145

I Draft of the catalogue of safety requirements according to §167 TKG

The measures set out in the catalogue of safety requirements are regularly reviewed and adapted to keep pace with the state of the art.

This draft includes the General Order of the Catalogue of Security Requirements under Section A, the actual Catalogue of Security Requirements under Section 167 of the Telecommunications Act under Section B, and an annex to the technical specification for packet-switched networks to the Catalogue of Security Requirements under Section C.

A General order

Pursuant to Section 167(1), first sentence, of the Telecommunications Act (TKG), the Federal Network Agency for Electricity, Gas, Telecommunications, Posts and Railways (Bundesnetzagentur) shall, in agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information:

1. The catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data, as set out in Section B, together with the Annex (Technical specification for packet-switched networks) in Section C, shall enter into force upon notification.
2. Within the implementation period pursuant to Section 167(3) of the Telecommunications Act, the obligations arising from the catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data issued by General Order No 63/2021 of 29 April 2020 (Security Catalogue Version 2.0) shall continue to apply to the addressees pursuant to Section 1 if the addressees pursuant to Section 1 fall within the scope of the Safety Catalogue Version 2.0 and if the addressees pursuant to Section 1 have not yet complied with the requirements of the Catalogue 1.

The catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data adopted by General Decision No 63/2021 of 25 August 2021 (OJ BNetzA No 16/2021) of 29 April 2020 (Security Catalogue Version 2.0), as last amended by General Decision No 57/2022 of 29 June 2022 (OJ BNetzA No 12/2022), is revoked with effect from DATE (entry into force SiKa-neu plus one year).

3. On the basis of point 3 of the first sentence of Paragraph 167(1) of the TKG, the various hazard potentials of public telecommunications networks and publicly accessible telecommunications services are determined in agreement with the BSI and the BfDI as follows:
 - a) **Normal hazard potential:** A provider of publicly available telecommunications services or a provider of public telecommunications networks has a normal risk potential if it employs fewer than 10 persons and its annual turnover or balance sheet total does not exceed EUR 2 million.
 - b) **Increased risk potential:** A provider of publicly available telecommunications services or an operator of public telecommunications networks has a higher risk potential if it is important for the public good. In any case, it has a higher risk potential if it:
 - i) employs fewer than 50 people; and
 - ii) has an annual turnover or annual balance sheet total of EUR 10 million or less.
 - c) **Increased risk potential:** A provider of publicly available telecommunications services or a provider of public telecommunications networks has an increased risk potential, provided that it is of paramount importance for the public good.

There is an increased risk potential in these cases:

- i) Operator of a public mobile network of the 5th Generation (5G network)
- ii) operators of other public telecommunications networks or providers of publicly available telecommunications services, if they:
 - (1) employs at least 50 people; or
 - (2) has an annual turnover and an annual balance sheet total of more than EUR 10 million each; or
 - (3) is an operator of critical installations in accordance with Section 2(1) of the German Roofing Act for Strengthening the Physical Resilience of Critical Installations (KRITISDachG).

For those undertakings with an increased risk potential, the table in Figure 2 of Chapter 1 of Annex 2 (Section D) shall apply: List of defined critical functions, § 167(1)(2) TKG.

The Bundesnetzagentur points out the following:

1. Pursuant to the third sentence of Paragraph 210 of the TKG in conjunction with the fourth sentence of Paragraph 41(4) of the VwVfG, **this order is deemed to have been made public on the date** of its publication on the website of the Bundesnetzagentur and its publication in the Official Journal of the Bundesnetzagentur. It thus enters **into force on the DATE.**
2. Obligated entities shall comply with the requirements of the Catalogue no later than one year after its entry into force. Under Paragraph 167(3) of the TKG, the transposition period is, in principle, one year. Under the second half-sentence of Paragraph 167(3) of the TKG, that period may be waived; In the present case, however, the Federal Network Agency does not exercise its discretion to derogate from such a derogation. The specifications of the catalogue are a further development of well-known standards and have already been established to a large extent, so that the implementation of the requirements can be mastered in one year.
3. The full decision will be published on the website of the Federal Network Agency.

Reasons:

I.

By General Decree No 63/2021, a catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data (security catalogue version 2.0) was adopted on 25 August 2021. In the course of the 2021 amendment to the TKG, the provisions on public security pursuant to §§ 165 et seq. of the TKG were partially recast, so that an adjustment to the legal requirements was necessary. To this end, the Federal Network Agency, in agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information, has drawn up the catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data as a basis for the security concept in accordance with § 167(1) TKG. The Safety Requirements Catalogue is hereinafter referred to as the 'Safety Catalogue'.

II.

1. Legal basis and formal legality (paragraphs 1 to 3) of the operative part)

The legal basis for issuing the safety catalogue is Paragraph 167(1) of the TKG. Any person who provides or participates in telecommunications services must take appropriate technical precautions and other measures in accordance with the first sentence of Paragraph 165(1) of the TKG. The details of the technical precautions and other measures to be taken pursuant to § 167(1)(1) TKG in conjunction with § 165(1) to (7) TKG shall be laid down by the Federal Network Agency (BNetzA) in agreement with the BSI and the BfDI by means of a general order in a catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data. More specifically:

- Section 167(1), first sentence, point 1, of the Telecommunications Act: details of the technical precautions and other measures to be taken pursuant to Section 165(1) to (7) of the Telecommunications Act, taking into account the various risk potentials of public telecommunications networks and publicly accessible telecommunications services,
- Section 167(1), first sentence, point 2, of the Telecommunications Act: which functions are critical functions performed by critical components within the meaning of Section 2(23) of the BSI Act (BSiG); and
- Section 167(1), second sentence, of the Telecommunications Act: The safety catalogue may also include requirements for the disclosure and interoperability of network component interfaces, including technical standards to be complied with.

Pursuant to the first sentence of Paragraph 167(1) of the TKG, this safety catalogue is an administrative act in the form of a general order pursuant to the second sentence of Paragraph 35 of the VwVfG.

On 19 November 2025, the Federal Network Agency published the draft safety catalogue in the Official Journal of the Federal Network Agency (22/2025) and on the website of the Federal Network Agency (<https://www.bundesnetzagentur.de/sicherheitsanforderungen>). Market participants had the opportunity to comment on the draft within one month. In so doing, the Bundesnetzagentur gave manufacturers, associations of operators of public telecommunications networks and associations of providers of publicly available telecommunications services the opportunity to submit their observations pursuant to the third sentence of Paragraph 167(1) of the TKG.

The legal basis for the revocation of the security catalogue version 2.0 (point 2) of the operative part) results from § 49(1) VwVfG (revocation of a lawful administrative act).

2. Substantive legality (paragraph 1) of the operative part)

The safety catalogue contains the main factual and legal reasons for the decision pursuant to the second sentence of Paragraph 39(1) of the VwVfG. The points of discretion are mentioned (§ 39(1) sentence 3 VwVfG).

Under Paragraph 165(1)(1)(1) **of the TKG, the addressees** of the general order are all those who provide or participate in telecommunications services. In addition, Paragraph 165(2)(2) of the TKG covers operators of public telecommunications networks and providers of publicly available telecommunications services.

Paragraph 3(61) of the TKG defines telecommunications services as services normally provided for remuneration over telecommunications networks, which, with the exception of services providing content over telecommunications networks and services or exercising editorial control over them, include the following services:

- d) Internet access services;
- e) interpersonal telecommunications services; and
- f) services consisting wholly or mainly in the transmission of signals, such as transmission services used for machine-to-machine communication and broadcasting.

This new definition, which is a transposition of Article 2(4)¹ of the EECC, means that a wider group of addressees is now covered than before. In particular, number-independent interpersonal telecommunications services are now also obliged to take technical precautions and other measures to protect telecommunications secrecy and against personal data breaches. This is due to the growing importance of these services.²

The new addressees providing number-independent interpersonal communications services usually do not exercise effective control over signal transmission over networks. Therefore, the

¹ BT-Drs. 19/26108, p. 236.

² EECC, recital 95.

European legislator classifies the risk for such services as ‘in some respects [...] lower’ than for traditional electronic communications services³:

*Therefore, where justified on the basis of the actual assessment of existing security risks, measures taken by providers of number-independent interpersonal communications services should be less stringent. The same approach should apply mutatis mutandis to interpersonal communications services using numbers that do not exercise effective control over signal transmission.*⁴

In addition, the requirements of the catalogue for the protection of telecommunications secrecy and personal data (§ 165(1) TKG) include those involved in the provision of services, i.e., for example, employees and vicarious agents. In addition, e.g. resellers who collect and use data for their customer management and accounting are recorded. This is done against the background that these providers also collect personal data and, if necessary, obtain information that is subject to telecommunications secrecy (invoicing, business figures).⁵ By contrast, the provision does not cover manufacturers of network components or terminal equipment.⁶

This large group of addressees is divided into the following three categories in the safety catalogue, which depend on the respective hazard potential. The safety catalogue provides for the following categories:

- Normal hazard potential
- Increased risk potential
- Increased risk potential

Depending on how the addressees are classified, they meet the obligations to varying degrees.

Addressing therefore takes place twice; once for the general classification in the circle of all obliged entities and a second time for the classification in the respective category.

II Scope of the regulatory effect (Section 35(1) of the VwVfG) and specificity (Section 37(1) of the VwVfG)

The legislature provides that the safety catalogue is to be issued as a general order, Section 167(1), first sentence, of the Telecommunications Act. The Safety Catalogue provides the basis for technical and organisational protection measures to be taken by providers and their contributors to telecommunications services. Both the range of possible obliged entities and possible technical measures is very wide. The safety catalogue regulates the following areas:

2) The entire group of addressees

³ EECC, recital 95.

⁴ EECC, recital 95. Although recitals themselves are not binding, they can be used in the context of teleological interpretation.

⁵ Sacks/Körber/Mozek, 4. ed. 2023, TKG § 165.

⁶ BT-Drs. 19/26108, p. 360.

- 3) The categorisation of the addressees by specifying the hazard potential of public telecommunications networks and publicly accessible telecommunications services as follows:
 - a) Normal hazard potential
 - b) Increased risk potential
 - c) Increased risk potential
- 4) Defining protective measures that must be implemented when the safety concept is drawn up
- 5) Definition of protective measures to be taken into account (but not necessarily implemented) in the preparation of the safety concept

When establishing protective measures, the safety catalogue can also only specify safety objectives, as is apparent from Section 166(1)(3)(c)(2). Half-sentence TKG results.

Non-compliance with the safety catalogue may be subject to a periodic penalty payment pursuant to Section 183(1) and (5) of the Telecommunications Act; in extreme cases, a prohibition order is possible, § 183(4) TKG. If the addressees fail to submit their safety concept, which is based on the safety catalogue, in full and in good time (§ 166(2) sentence 1, paragraph 4 sentence 2 TKG), § 228(2) numbers 3c and 38 TKG are also relevant in addition to § 183 TKG. This is an administrative offence that can be punished with a fine of up to EUR 300,000.

The catalogue may therefore be drawn up in accordance with Section 166(1)(3)(c)(2). HS TKG on the one hand only define objectives; on the other hand, its non-enforcement may lead to periodic penalty payments or fines, so that the addressee must be clearly defined. The catalogue must clearly state whether a measure is directly binding or 'only' has to be taken into account when drawing up the safety concept. In the latter case, non-implementation must be documented accordingly by the addressees.

For the content to **be precise, it is sufficient** that sufficient clarity can be gained from the entire content of the administrative act and from the context, in particular from the reasons given by the authority and from the more detailed circumstances of the adoption known to the parties, by means of an interpretation based on the principles of good faith.⁷ In accordance with Section 133 of the German Civil Code (BGB), the declared intention must be taken into account from the point of view of an informed recipient.⁸

The safety catalogue clearly indicates to the addressees under which level of hazard potential they fall. It is still clearly defined which measures they have to implement and which they only have to take into account.

⁷ VGH Mannheim Urt. v. 6.11.2013 - 1 S 1640/12, BeckRS 2013, 58560, beck-online mwN.

⁸ VGH Mannheim Urt. v. 6.11.2013 - 1 S 1640/12, BeckRS 2013, 58560, beck-online mwN.

III Indeterminate legal concepts

On the factual side, the individual provisions of § 165 TKG provide for indeterminate legal concepts (e.g. 'adequate technical and organisational precautions', 'other measures', 'significant impairments', 'state of the art'), which must be specified in more detail by the Federal Network Agency through the safety catalogue. The third sentence of Paragraph 165(2) of the TKG refers to the 'state of the art' when drawing up the safety concept. The term is mentioned in the second sentence of Paragraph 165(1) and the third sentence of Paragraph 165(2) of the TKG. The Handbook of Legal Formality of the Federal Ministry of Justice provides details on the interpretation of the term.⁹

Thus, in general, the legislator should use only the following general clauses for technical rules:

- generally accepted rules of technology,
- state of the art and
- State of Science and Technology.

Which of the three basic forms is to be chosen depends on the **hazard potential** of the matter, which is to be regulated, and on the technical controllability of this hazard potential.¹⁰

The manual goes on to say:

*The general clause 'generally **accepted rules of technology**' is used for cases with comparatively **low risk** potential or for cases that are technically manageable on the basis of proven experience. Generally accepted rules of technology are technical examples fixed in writing or handed down orally: The reference standard is null and void in the absence of legislative competence; however, the basic rule has been adopted in accordance with competence. The defect in the reference standard is irrelevant to the original standard. Provisions for procedures, facilities and operating methods which, according to the prevailing opinion of the parties involved (professionals, users, consumers and public authorities), are suitable for achieving the legally prescribed goal and which have generally proven themselves in practice or whose probation is, according to the prevailing opinion, imminent in a manageable time.¹¹*

*The level of requirements for the general clause 'state **of the art**' lies **between** the level of requirements for the general clause 'generally **accepted rules of the art**' and the level of requirements for the general clause 'state **of science and technology**'. **The state of the art is the level of development of advanced procedures, facilities and methods of operation which, according to the prevailing opinion of leading experts, makes it appear certain that the legally prescribed objective will be achieved.** Procedures, facilities and operating methods or similar procedures, facilities and operating methods must have proven themselves in practice or, if not already the case, should have been successfully*

⁹ Handbook of Legal Formality of the Federal Ministry of Justice, para. 252 et seq.

¹⁰ Handbook of Legal Formality of the Federal Ministry of Justice, para. 252.

¹¹ Handbook of Legal Formality of the Federal Ministry of Justice, paragraph 255.

tested in operation if possible. European Union law also uses the term ‘best available techniques’. This is largely in line with the ‘state of the art’ general clause.¹²

*The general clause ‘State of Science and Technology’ defines the **highest** level of requirements and is therefore used in cases with very high risk potential. The state of the art in science and technology is the state of development of the most advanced procedures, facilities and methods of operation which, in the opinion of leading experts in science and technology, on the basis of the latest scientifically justifiable findings, are deemed necessary in view of the legally prescribed objective and make it appear certain that this objective will be achieved’.¹³*

IV Exercise of discretion

1.1.1 Resolution discretion

Paragraph 167(1) of the TKG provides that the Federal Network Agency, in agreement with the BSI and the BfDI, is to adopt a catalogue of security requirements in the form of a general order. In that regard, the legislature does not provide for a discretionary resolution. In terms of content, however, there is a resolution discretion in two places:

1. The fifth sentence of Paragraph 165(3) of the TKG provides that the Federal Network Agency may lay down details of intrusion detection systems in the security catalogue;
2. Paragraph 167(1), second sentence, of the TKG: The catalogue of security requirements may include requirements for the disclosure and interoperability of network component interfaces, including technical standards to be complied with.

Point 4.9.1 of the Security Catalogue contains an explanation of attack detections; he also mentioned the point of interoperability at various points, without imposing any further requirements in this regard at this stage.

1.1.2 Selection fairs

The Federal Network Agency also has a selection fair.

As already stated, the content of the safety catalogue is very extensive, as it must cover a considerable range of addressees and possible issues. In addition, there is the constant development of technology. As already explained above, the Safety Catalogue provides that the Federal Network Agency further specifies the indeterminate legal concepts from § 165 TKG. In determining the ‘details of the technical precautions and other measures to be taken pursuant to Section 165(1) to (7) of the Telecommunications Act, taking into account the various risk potentials’, the Federal Network Agency has a discretion on the legal consequences side.

The safety catalogue shall specify the appropriate technical precautions and other measures to be taken by the addressees. This is to a large extent a creative activity in which the authorities have to weigh the security concerns of the population and the functioning of the state against the freedom of occupation of the addressees. For this purpose, the Federal Network Agency selects from a large number of possible technical options those that best reconcile the

¹² Handbook of Legal Formality of the Federal Ministry of Justice, para. 256.

¹³ Handbook of Legal Formality of the Federal Ministry of Justice, para. 257.

regulatory objectives of § 2(2) TKG. This is done against the background of a dynamic threat situation, which is developing very quickly both politically and technically. In addition, there are no firmly binding technical standards for this prognostic decision.

The discretion allows a margin of discretion, in the exercise of which the Federal Network Agency is guided by the **regulatory objectives** set out in Paragraph 2(2) of the TKG. In the present case, the Bundesnetzagentur promotes the interests of users by safeguarding the interests of public security and ensuring the security of networks and services (Paragraph 2(2) (3) of the TKG). These requirements are further differentiated in the definitions in § 3 No. 52 TKG. This standard defines 'network and service security' as the ability of telecommunications networks and services, at a certain level of trust, to defend against all attacks that affect:

- availability;
- authenticity;
- Integrity
- or confidentiality

those networks and services, the data stored, transmitted or processed or the related services offered or accessible through those telecommunications networks or services.

1.1.3 No misuse of judgement: General considerations of proportionality with regard to all measures mentioned in the catalogue

Since there is a discretion, the Federal Network Agency is obliged under § 40 VwVfG to exercise its discretion in accordance with the purpose of the authorisation and to comply with the legal limits of the discretion. In adopting the present administrative act, it observes, in particular, proportionality in the context of interference with fundamental rights. The purpose of the authorisation is, in particular, the protection of telecommunications secrecy and the protection of personal data (Section 165(1), first sentence, of the Telecommunications Act).

(1) Incriminating administrative act: Interference with the scope of protection of Article 12(1) of the Basic Law

In particular, the obligations arising from the safety catalogue may interfere with the freedom to choose an occupation under Article 12(1) of the Basic Law. For example, the measures entail costs that are lacking elsewhere for investments; Depending on the scale and cost of the measures, a barrier to entry may arise for new entrants. Smaller companies may be forced to leave the market. Employees must also be trained. Depending on the offer of the certifiers, necessary certifications may not be obtained immediately, even if all requirements are met; in addition, staff must be employed or re-hired for the security measures.

Under the first sentence of Article 12(1) of the Basic Law, all Germans have the right to freely choose their profession, place of work and place of training. Pursuant to the second sentence of Article 12(1) of the Basic Law, the practice of the profession may be regulated by law or on the basis of a law.

Under Article 19(3) of the Basic Law, the freedom to choose an occupation also applies to domestic legal persons in so far as it is by its nature applicable to them. For the domestic

criterion, the seat theory is decisive, i.e. whether the effective (actual) seat¹⁴ is in Germany (or, according to an interpretation in conformity with European law, in the EU).¹⁵ Internationally active legal persons have their head office in Germany only if the majority of management decisions in Germany are also taken.¹⁶ Undertakings which are not established in Germany within the meaning of an action centre may only claim subsidiary protection under Article 2(1) of the Basic Law. However, if such an undertaking from a third country establishes a subsidiary which has at least partial legal capacity and which has its action centre in Germany, that part of the undertaking is protected domestically and in accordance with Article 12(1) of the Basic Law.¹⁷ The registered office shall be determined separately for each legal person.¹⁸

The **intensity of the intervention** was **concretized by the Federal Constitutional Court with the help of the 3-step theory**.¹⁹

The **1st The stage** (professional rules) concerns the ‘how’ of the exercise of the profession and is justified. They do not concern the question of who may exercise it and under what conditions; therefore, those rules are already justified if they properly protect reasonable public interest interests.

Subjective rules on career choice (**2. Stage**) concerns the ‘whether’ of the exercise of the profession, whereby entry requirements for certain professions are linked to subjective criteria. Access to the profession thus depends on certain factors inherent in the person and thus capable of being influenced; this includes, for example, evidence of qualifications or personal reliability.

Such rules are permissible if they are necessary to protect an important, particularly important or outstandingly important common good.

Objective rules for choosing a profession (**3. Level**) link access to the profession to **criteria outside the person**. This includes, for example, demand regulations or protection against competition. These measures are justified if they are intended to ‘defend demonstrable or highly probable serious dangers to an extremely important common good’.

The Safety Catalogue regulates the ‘how’ and ‘whether’ of the exercise of the profession and thus refers to the **1st and 2nd Step** into the freedom to choose an occupation. In order for the interference to be proportionate, the arrangements must at least be necessary to protect an important common good.

(2) Proportionality of the interference

Legitimate purpose

¹⁴ Dürig/Duke/Scholz/Remmert, 103. EL January 2024, GG Article 12(1), paragraph 69.

¹⁵ Threesome/threesome, 3. ed. 2013, GG Art. 19 III para. 79.

¹⁶ BeckOK GG/Enders, Beck’scher Online-Kommentar GG, 36. Ed. 15.2.2018, Art. 19, para. 36; Threesome/threesome, 3. ed. 2013, GG Art. 19 III para. 79.

¹⁷ Dürig/Duke/Scholz/Remmert, 103. EL January 2024, GG Art. 12(1) para. 66.

¹⁸ Ludwigs/Friedman, The Right to Fundamental Rights of Legal Persons according to Art. 19 III GG, JA 2018, 807 (807 ff.).

¹⁹ Pharmacy judgment, BVerfGE 7, 377, paragraph 62 et seq., paragraph 72 et seq.

The legal basis for the safety catalogue is § 167(1) in conjunction with § 165 TKG. According to Paragraph 165(1)(1) and (2) of the TKG, a central purpose of the catalogue is the protection of telecommunications secrecy. In this respect, it is a simple-law formulation of the state protection obligations under **Article 10 of the Basic Law** (telecommunication secrecy) and **Article 2(1) in conjunction with Article 1(1) of the Basic Law** (general right of personality).

With regard to the regulatory objectives, the safety catalogue promotes the interests of users by the Federal Network Agency safeguarding the interests of public safety and ensuring the safety of networks and services (§ 2(2)(3) TKG).

However, the security requirements do not only protect the individual; Since telecommunications and data processing systems are now used in all critical areas of the state, failure there may affect the security and functioning of the state and its facilities. This essentially concerns the constitutional structural principles set out in **Article 20(1) to (3) of the Basic Law**. That objective can be found, by simple law, in Paragraph 165(2) of the TKG (protection against disruptions leading to significant impairments of telecommunications networks and -services) and Paragraph 165(5) of the TKG (ensuring the proper operation of networks).

In addition, a failure of the telecommunications and data processing systems to be protected by the security requirements may result in commercial customers of the company being affected in their property and professional rights (**Article 12(1), Article 14(1) of the Basic Law**). The company concerned is also protected by the security measures; in addition to self-protection, the fact that the entire industry adheres to a uniform level of protection and that the purchase of services is also subject to the safety standard. Due to the interdependencies, providers affected by the security catalogue are regularly themselves users of such services with other providers. Against this background alone, a uniform level of protection is necessary; otherwise, a weak security concept could 'cross' from one provider to the next and affect their freedom to pursue their profession.

Measures such as redundant hardware and backups not only protect against attacks, but also against other failures.

Appropriateness

The measures in the safety catalogue must be specifically suitable for achieving the above-mentioned safety objectives, i.e. they must at least be conducive to achieving the objectives. The measures are at least conducive to achieving the objective of the security of networks and services and are therefore appropriate.

Necessity

Nor are there any more lenient means that would be equally suitable for achieving the objective.

The security catalogue covers a wide range of addressees and possible issues. It affects both very large companies that operate highly safety-critical infrastructure and smaller companies that have less financial resources but are not equally vulnerable.

The safety catalogue takes this range into account by dividing the addressees into different categories depending on their risk potential. This is already laid down in the Act (Paragraph 167(1), first sentence, point 1, of the TKG: ‘taking into account the various hazard potentials’).

Appropriateness (proportionality i.e.S.)

The measure is also appropriate as the intended purpose is not disproportionate to the seriousness of the interference. The appropriateness of the measures from the safety catalogue depends on various criteria. At the level of European law, Article 21(1) of the second subparagraph of Article 21(2) of the NIS2 Directive can first be used here. It reads as follows:

*The measures referred to in the first subparagraph shall ensure a level of security of network and information systems commensurate with the existing risk, taking into account **the state of the art and, where appropriate, the relevant European and international standards and the costs of implementation. When assessing the proportionality of those measures, due account shall be taken of the level of risk exposure of the entity, the size of the entity and the likelihood of incidents occurring and their severity, including their societal and economic impact.***

Under the first sentence of Paragraph 165(6) of the TKG, technical precautions and other protective measures are appropriate if the technical and economic effort required is not disproportionate to the importance of the telecommunications networks or services to be protected.

In general, it can therefore be stated that **scalable systems** that can be adapted to the individual network operator and take into account its size and system relevance speak in favour of appropriate measures.²⁰

The security catalogue scales both with regard to the addressees and with regard to the measures to be taken. On the one hand, the addressees are divided according to risk potential in order to prevent non-risk-relevant business activities from being disproportionately burdened. On the other hand, in addition to the mandatory measures, the safety catalogue also contains measures that must be taken into account when drawing up the protection concept; where appropriate, the addressee may also derogate from those measures.

Addressees

The group of addressees is already defined by the legislator. The classification of the addressees on the basis of the potential risks is also already laid down in the Act (Section 167(1), first sentence, point 1, of the Telecommunications Act: ‘taking into account the various hazard potentials’).

²⁰ Düsseldorf Higher Regional Court decision of 19 July 2017 – 3 kart 109/16, BeckRS 2017, 132865 paragraph 58, beck-online on the adequacy of the IT security catalogue pursuant to § 11(1a) EnWG.

In the safety catalogue of micro-enterprises, the Federal Network Agency has classified micro-enterprises separately under 'normal' risk potential in order to make the obligations as appropriate as possible to the risk. However, even if the addressees fall under a higher risk potential, this does not mean that safety concerns automatically take precedence over the other balancing concerns as part of the balancing exercise.

Obligations for addressees of the respective categories

In exercising its discretion, the Bundesnetzagentur weighs up the protected assets referred to in the regulatory objectives set out in Paragraph 2(2) of the TKG. The security catalogue serves to safeguard the interests of public security and to ensure the security of networks and services (Section 2(2)(3)(c) TKG). It should be noted that absolute safety cannot be achieved; In principle, further security measures are still possible.²¹ However, the Federal Network Agency also has the task **of ensuring equal opportunities for competition** (Section 2(2)(2) of the Telecommunications Act). Against this background, the security requirements must not create a barrier to entry or oblige the incumbent competitor to leave the market. When weighing profitability and/or cost-effectiveness against safety considerations, it makes sense to aim at a level of safety that guarantees the functionality of the infrastructure against normally expected hazards.

It should also be noted that the security measures also benefit the addressees themselves. The measures protect their safe practice, not only in terms of protection against attacks, but also in the event of other data loss.

In order to limit the additional costs for market participants, the safety catalogue is based on industry standards (see Section 6.2 of the safety catalogue).

This also complies with the requirements of Article 21(5) UA 3 of the NIS2 Directive, which is addressed to the European Commission:

*When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, as far as possible, **follow European and international standards and relevant technical specifications.** [...]*

Adopting European and international standards and relevant technical specifications as uniformly as possible facilitates implementation and contributes to the functioning of the European internal market. Since the safety catalogue is now embedded in European law, there is no competitive disadvantage for market participants in Germany compared to European competitors.

The adequacy of each measure shall be determined on the basis of an analysis of the protection needs.²² In particular, the following factors are conceivable:²³

- The interest of third parties in becoming aware;

²¹ Geppert/Schütz/Eckhardt, 5. ed. 2023, TKG § 165 para. 55.

²² Geppert/Schütz/Eckhardt, 5. ed. 2023, TKG § 165 para. 55.

²³ Geppert/Schütz/Eckhardt, 5. ed. 2023, TKG § 165 para. 55.

- possible misconduct or abuse by own employees;
- the level of access barriers to be overcome in each case; and
- costs through technical and organisational safeguards.

When issuing the safety catalogue, the Federal Network Agency also ensured legal certainty for operators. Within the framework of the individual measures, it is clear to the addressees which further processes are required to meet the requirements. This concerns in particular the security clearance of third parties.

Finally, the **dynamic development of technologies** must also be taken into account. Newly developed network and system components must be able to be tested and certified immediately. Here, care is taken that the certification bodies do not delay the use of new components. Section B, point 5.2, of the catalogue provides for the certification of critical components on the basis of the BSI TR-03163. In addition, there are transitional arrangements for the certification of critical components, arrangements for existing components and a cut-off date.

1.1.4 Revocation of the security catalogue version 2.0 (point 2) of the operative part)

The requirements for the revocation of the security catalogue version 2.0 from § 49(1) of the Administrative Procedure Act are met. In particular, the new security catalogue is not an administrative act of the same content.

1.1.5 Separate considerations of legality relating to the potential risks (paragraph 3) of the operative part)

Chapter 3 of the Safety Requirements Catalogue further defines the various hazard potentials of public telecommunications networks and publicly accessible telecommunications services in order to subsequently define appropriate protective measures according to the respective hazard potential. Depending on which category a company falls into, the level of interference with fundamental rights varies. In this chapter, the addressees of the security catalog are again divided into three different groups. The classification determines which protective measures from Chapters 4 and 5 apply to the addressees.

The classification as such serves to ensure the scalability of the measures so that the interference with fundamental rights can be kept as low as possible. This is already laid down in the Act (Paragraph 167(1), first sentence, point 1, of the TKG: 'taking into account the various hazard potentials'). The safety catalogue provides for the following categories:

- Normal hazard potential
 - o less than 10 employees; and
 - o maximum annual turnover or annual balance sheet total of EUR 2 million
 - o Consequence: Classification as other public telecommunications networks and publicly available telecommunications services

- Increased risk potential
 - o less than 50 employees; and
 - o maximum annual turnover of EUR 10 million or annual balance sheet total
 - o Consequence: classification as public telecommunications networks; and publicly available telecommunications services that are important for the common good
- Increased risk potential
 - o at least 50 employees, or
 - o more than EUR 10 million in annual turnover and annual balance sheet total, or
 - o Operators of critical installations according to § 2 No. 1 Roofing Act to strengthen the physical resilience of critical installations (KRITISDachG)
 - o Consequence: Classification as public telecommunications networks and publicly available telecommunications services of high importance for the common good
 - o An increased risk potential also results from the operation of a mobile network of the 5. Generation (5G network).

According to Section 28(3) of the BSIG, business activities that are negligible with regard to the entire business activity of the institution may not be taken into account when classifying them into the various risk potentials.

According to § 28(4) sentence 2 BSIG, the data of partner or affiliated companies are not to be added if the company is independent of its partner or affiliated companies, taking into account the legal, economic and factual circumstances with regard to the nature and operation of the information technology systems, components and processes.

These indicators are also appropriate. The criteria 'number of employees' and 'economic indicators' can be used to draw conclusions about the quantity and quality (importance) of customers. The importance for the common good thus arises either from the fact that a significant proportion of the population uses the service itself and/or that a customer uses the service, which in turn is important for the common good. If a customer is important for the common good, his failure is accordingly also safety critical for the common good.

The type of use can also be derived from the above criteria. For example, if a company either has a large number of customers or the customers are critical to security, the services are typically kept redundant, which is reflected in the number of employees and pricing.

In addition, the criteria are objectively ascertainable and therefore provide legal certainty. The criteria are also well known and have also proven themselves in other, similar contexts for delimitation. They were already formulated in a Commission Recommendation in 2003, which

distinguished different micro, small and medium-sized enterprises (SMEs).²⁴ Although the delimitation is not directly found in the TKG, the criteria are mentioned several times in the adjoining regulations on information security.

Article 3 of the NIS2 Directive,²⁵ transposed into Paragraph 28 of the BSIG, defines essential and important institutions. Article 3(1)(a) of the NIS2 Directive refers to Annex I to that directive. Annex I to the Directive contains a list of different sub-sectors with strong criticality. However, in order for them to be regarded as essential entities, Article 3(1)(a) of the NIS2 Directive requires them to exceed the thresholds laid down in the SME Recommendation for medium-sized enterprises. In addition, it must be taken into account for micro-enterprises that the subdivision in § 28 BSIG into "particularly important institutions" and "important institutions" does not sufficiently take into account the economic effort in consideration of the lower risk of danger. Therefore, a more nuanced approach seems appropriate and therefore the SME recommendation underpinning the NIS2 Directive should also be used for micro-enterprises. Against this background, a further category with "normal risk potential" will be created for micro-enterprises within the framework of this safety catalogue.

Finally, it should be borne in mind that both the safety catalogue and the security concept based on it enable further scalability in order to avoid a disproportionate burden within the categories in individual cases.

In addition to the key figures and the number of employees, special features of the telecommunications network/service to be protected can also indicate a certain importance for the common good or at least further substantiate the assumption of a special importance. The public mobile network has a special position in this context. In the case of the mobile network, cross-sectional use in all areas of public life is to be assumed. The availability and security of this network is therefore highly likely to affect not only the individual, but the state, the economy and society alike. The operation of 5G networks within the meaning of EU-Recommendation 2019/534 of 26 March 2019 has an enormous special status. In this sense, 5G networks are the future backbone of our increasingly digitized economies and societies. They will connect billions of objects and systems and will also process sensitive information and support security systems in the critical infrastructures of the energy, water, food, health, finance and insurance, transport and transport sectors, as well as the information technology and telecommunications sectors. Therefore, if publicly accessible 5G mobile networks are operated, an outstanding importance of these telecommunications networks for the common good may be indicated.

²⁴ Article 2 of the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, reference number C(2003) 1422, Official Journal No L 124, 20/05/2003 p. 0036 – 0041; see also recital 4.

²⁵ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14. December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Instructions on remedies:

An objection to this general order may be lodged with the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, Tulpenfeld 4, 53113 Bonn or any other department of the Federal Network Agency within one month of notification.

An objection does not have suspensive effect pursuant to § 217(1) TKG.

B Catalogue of safety requirements §167 TKG

1. Introduction/General

In accordance with the first sentence of Paragraph 167(1) of the TKG, this catalogue of safety requirements (safety catalogue) lays down the following:

1. details of the technical precautions and other measures to be taken pursuant to Section 165(1) to (7) of the Telecommunications Act, taking into account the various risk potentials of public telecommunications networks and publicly accessible telecommunications services,
2. which functions are critical functions that are implemented by critical components § 2 No. 23 BStG.

These determinations will be made below. Manufacturers, associations of operators of public telecommunications networks and associations of providers of publicly available telecommunications services were involved in the preparation of the catalogue.

The details of the technical precautions and other measures to be taken pursuant to § 167(1) (1) TKG in conjunction with § 165(1) to (7) TKG shall be laid down by the Federal Network Agency (BNetzA) in agreement with the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) by means of a general order in a catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data.

For this purpose, § 165 TKG defines certain safety objectives and protective obligations. First of all, Paragraph 165(1) of the TKG obliges providers of telecommunications services and those involved to take appropriate technical precautions and other measures to protect telecommunications secrecy and against breaches of the protection of personal data. In addition, pursuant to Paragraph 165(2) of the TKG, operators of public telecommunications networks and providers of publicly available telecommunications services are required to protect the telecommunications and data processing systems operated against disruptions that lead to significant impairments of telecommunications networks and services, even if such disruptions may be caused by external attacks and the effects of disasters, and to take appropriate technical and organisational measures and other measures to control the risks to the security of telecommunications networks and services.

This catalogue is based on ENISA's 'Guideline on security measures under the EEC' (status: 07/2021)²⁶.

If telecommunications law obligations under §§ 165 and 166 TKG are fulfilled by other persons or bodies on behalf of a person responsible and data is processed in this context, the obliged entity must ensure compliance with telecommunications law provisions. This does not affect the direct data protection responsibility of the commissioned person or body under general data protection law.

²⁶ <https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc>

Pursuant to Section 165(9) of the Telecommunications Act, the Federal Network Agency (BNetzA) may require operators of public telecommunications networks or providers of publicly available telecommunications services to submit to a review by the Federal Office for Information Security or a qualified independent body designated by it, on the basis of which the Federal Office for Information Security shall determine whether the requirements laid down in paragraphs 1 to 7 have been infringed.

In order to improve the control of risks for public telecommunications networks and publicly available telecommunications services, Section 166 of the Telecommunications Act provides for the establishment of a security concept, the designation of a security officer and the designation of a contact person established in the European Union.

Note:

In fulfilling his obligations under telecommunications law, the obliged entity must also comply with the general data protection requirements of the Federal Data Protection Act (BDSG), the Telecommunications Digital Services Data Protection Act (TDDDG) and the General Data Protection Regulation (GDPR).

It must be borne in mind here that, on the basis of Article 95 of the GDPR, Paragraph 165 of the TKG, as a transposition of the ePrivacy Directive, takes precedence over the comparable provisions of the GDPR (in particular Article 32), in so far as they pursue the same objective. Further information can be found in Chapter 4.1.

2. addressee

The catalogue of safety requirements specifies the technical precautions and other measures to be taken pursuant to § 165(1) to (7) TKG and is aimed at all relevant companies within the scope of the TKG (§ 1(2) TKG).

The addressees of Paragraph 165(1) (also in conjunction with Paragraphs 6 and 7) of the TKG are all providers of telecommunications services and contributors thereto. The addressees of Paragraph 165(2) and (3) (also in conjunction with Paragraph 165(6) and (7)) of the TKG are operators of public telecommunications networks and providers of publicly available telecommunications services. The addressees of Paragraph 165(4) and (5) (also in conjunction with Paragraph 165(6) and (7)) of the TKG are operators of public telecommunications networks.

According to § 3 No. 7 TKG, the operator is an undertaking which provides or is authorised to provide a public telecommunications network or an associated facility.

According to § 3 No. 1 TKG, the provider of telecommunications services is anyone who provides telecommunications services.

The obligations arising from the second and fourth sentences of Paragraph 165(3) of the TKG are addressed only to operators of public telecommunications networks and providers of publicly available telecommunications services who are particularly important entities within the meaning of point 3 of the first sentence of Paragraph 28(1) of the BStG. The various hazard potentials are defined in Chapter 3 below.

3. Determination of hazard potentials

The security concept to be drawn up pursuant to Paragraph 166(1)(3) of the TKG must indicate the hazards to be assumed and the technical precautions and other measures to be implemented in compliance with the various hazard potentials of public telecommunications networks and publicly accessible telecommunications services. The risks are directly dependent on the importance of networks and services. The importance of the telecommunications network or service to be protected is therefore decisive for its risk potential. In principle, public telecommunications networks and services can be assigned to the following hazard potentials:

- **Normal hazard potential:** All public telecommunications networks and publicly available telecommunications services
- **Increased risk potential:** Public telecommunications networks and publicly available telecommunications services, where they are important for the public interest
- **Increased risk potential:** Public telecommunications networks and publicly available telecommunications services, provided that they are of paramount importance for the common good

3.1 Hazard potentials

Pursuant to § 167(1) sentence 1 number 1 TKG, the various hazard potentials of public telecommunications networks and publicly accessible telecommunications services are defined in agreement with the BSI and the BfDI as follows:

- **Normal hazard potential:** From a constitutional point of view, the importance of the legal interests to be protected by § 165 TKG (telecommunication secrecy, protection of personal data and functionality of telecommunications networks and services) for the individual must be taken into account. A normal risk potential must therefore at least be based on this significance and ensure compliance with corresponding precautions and other protective measures.

A provider of publicly available telecommunications services or a provider of public telecommunications networks has a normal risk potential if it employs fewer than 10 persons and its annual turnover or balance sheet total does not exceed EUR 2 million.

- **Increased risk potential:** A provider of publicly available telecommunications services or an operator of public telecommunications networks has a higher risk potential if it is important for the public good.

In any case, it has a higher risk potential if it:

- a) employs fewer than 50 people; and
- b) has an annual turnover or annual balance sheet total of EUR 10 million or less;

- **Increased risk potential:** A provider of publicly available telecommunications services or a provider of public telecommunications networks has an increased risk potential, provided that it is of paramount importance for the public good.

In any case, there is an increased risk potential in these cases:

- a) Operator of a public mobile network of the 5th Generation (5G network)
- b) operators of other public telecommunications networks or providers of publicly available telecommunications services, if they:
 - i) employs at least 50 people; or
 - ii) has an annual turnover and an annual balance sheet total of more than EUR 10 million each; or
 - iii) is an operator of critical installations in accordance with § 2 No. 1 KRITISDachG.

Pursuant to § 167(1)(1) TKG, BNetzA shall, in agreement with the BSI and the BfDI, lay down details of the technical precautions and other measures to be taken pursuant to § 165(1) to (7) TKG, taking into account the various risk potentials of public telecommunications networks and publicly accessible telecommunications services. The importance of networks and services and the different risk potentials give rise to different requirements for networks and services. In the telecommunications sector, there is a great diversity of telecommunications companies on the market. Therefore, obliged entities are expected to take only appropriate, necessary and proportionate technical precautions and other measures. Technical precautions and other protective measures are appropriate if the technical and economic effort required for this is not disproportionate to the importance of the telecommunications networks or services to be protected, § 165(6) sentence 1 TKG. The present catalogue of safety requirements is intended to make a significant contribution to the determination of the relevant technical precaution or other measure. The assessment of the individual case is the responsibility of the company concerned, taking into account the risk potential identified in each case.

Normal hazard potential: All operators of public telecommunications networks and providers of publicly available telecommunications services are subject to the normal risk potential. These must implement at least the basic protective measures of category (a) of the respective areas in Chapter 4 of the Safety Requirements Catalogue.

Increased risk potential: Operators of public telecommunications networks and providers of publicly available telecommunications services that are subject to the higher risk potential must implement at least the basic protection measures of category (a) and the extended protection measures of category (b) in Chapter 4 of the catalogue of security requirements of the respective areas in order to meet the security objectives.

Increased risk potential: Operators of public telecommunications networks and providers of publicly available telecommunications services that are subject to the increased risk potential within the meaning of case groups (a) or (b) must implement at least the basic protection measures of categories (a), the extended protection measures of category (b) and the full protection measures of category (c) in Chapter 4 of the catalogue of security requirements of the respective areas in order to meet the security objectives.

5G network operators under case group (a) shall also comply with the security requirements set out in Chapter 5 of the Security Requirements Catalogue.

3.2 Proportionality considerations for determining the hazard potentials

Chapter 3 of the Safety Requirements Catalogue further specifies the various hazard potentials of public telecommunications networks and publicly available telecommunications services in order to subsequently define appropriate protective measures according to the respective hazard potential. Depending on which category a company falls into, the level of interference with fundamental rights varies. In this chapter, the addressees of the security catalog are again divided into three different groups. The classification determines which protective measures from Chapters 4 and 5 apply to the addressees.

The classification as such serves to ensure the scalability of the measures so that the interference with fundamental rights can be kept as low as possible. This is already laid down in the Act (Paragraph 167(1), first sentence, point 1, of the TKG: 'taking into account the various hazard potentials'). Such a classification in this sense is already contained in the BSIG, whose category of "particularly important institutions" is explicitly referred to in § 165(3) TKG.

Entities which, in accordance with Article 2(3) of the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (SMEs), are "micro-enterprises" based on the following indicators:

- less than 10 employees; and
- Annual turnover or annual balance sheet less than EUR 2 million

divided.

Entities that are classified as "micro-enterprises" in accordance with Article 2(3) of the SME Recommendation are assigned to the "normal risk potential" within the framework of this safety catalogue.

Consequence: Classification as other public telecommunications networks and publicly available telecommunications services

The "important institutions" referred to in Section 28(2) BSIG are based on the following indicators:

- employs fewer than 50 people; and
- an annual turnover or balance sheet total of 10 million or less;

divided.

Institutions classified as "important institutions" in accordance with § 28(2) BSIG are assigned to the "high hazard potential" within the scope of this safety catalogue.

Consequence: Classification as public telecommunications networks and publicly available telecommunications services of greater importance for the common good

The "particularly important institutions" referred to in § 28(1) BSIg are based on the following indicators:

- at least 50 employees, or
- an annual turnover and an annual balance sheet total of more than 10 million euros each divided.

Institutions classified as "particularly important institutions" in accordance with § 28(1) BSIg are assigned to the "increased risk potential" within the framework of this safety catalogue.

Consequence: Classification as public telecommunications networks and publicly available telecommunications services of paramount importance for the common good

These indicators are also appropriate. The criteria 'number of employees' and 'economic indicators' can be used to draw conclusions about the quantity and quality (importance) of customers. The importance for the common good thus arises either from the fact that a significant proportion of the population uses the service itself and/or that a customer uses the service, which in turn is important for the common good. If a customer is important for the common good, his failure is accordingly also safety critical for the common good.

The type of use can also be derived from the above criteria. For example, if a company either has a large number of customers or the customers are critical to security, the services are typically kept redundant, which is reflected in the number of employees and pricing.

In addition, the criteria are objectively ascertainable and therefore provide legal certainty. The criteria are also well known and have also proven themselves in other, similar contexts for delimitation. They were already formulated in a Commission Recommendation in 2003 which differentiated between micro, small and medium-sized enterprises (SMEs).²⁷ Although the delimitation is not directly found in the TKG, the criteria are mentioned several times in the adjoining regulations on information security.

Article 3 of the NIS2 Directive²⁸ defines essential and important entities. Article 3(1)(a) of the NIS2 Directive refers to Annex I to that directive. Annex I to the Directive contains a list of different sub-sectors with strong criticality. However, in order for them to be regarded as essential entities, Article 3(1)(a) of the NIS2 Directive requires them to exceed the thresholds laid down in the SME Recommendation for medium-sized enterprises.

Finally, it should be borne in mind that both the safety catalogue and the security concept based on it enable further scalability in order to avoid a disproportionate burden within the categories in individual cases.

²⁷ Article 2 of the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, reference number C(2003) 1422, Official Journal No L 124, 20/05/2003 p. 0036 – 0041; see also recital 4.

²⁸ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14. December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

In addition to the key figures and the number of employees, special features of the telecommunications network/service to be protected can also indicate a certain importance for the common good or at least further substantiate the assumption of a special importance. The public mobile network has a special position in this context. In the case of the mobile network, cross-sectional use in all areas of public life is to be assumed. The availability and security of this network is therefore highly likely to affect not only the individual, but the state, the economy and society alike. The operation of 5G networks within the meaning of EU Recommendation 2019/534 of 26 March 2019 has an enormous special status. In this sense, 5G networks are the future backbone of our increasingly digitized economies and societies. They will connect billions of objects and systems and will also process sensitive information and support security systems in the critical infrastructures of the energy, water, food, health, finance and insurance, transport and transport sectors, as well as the information technology and telecommunications sectors. The operation of public 5G mobile networks or the provision of publicly available 5G telecommunications services therefore indicate that these telecommunications networks are of paramount importance for the common good.

4. Definition of basic details of the technical precautions and other measures to be taken, taking into account the various hazard potentials, § 167(1) (1) TKG

Information security management, or IS management for short, is the part of general risk management that aims to ensure the confidentiality, integrity and availability of information, business processes, applications and IT systems.

In order to achieve a needs-based level of security for all business processes, information and technology, suitable organizational and personnel framework conditions must also be created to a considerable extent.

The protective measures listed below address these aspects, taking into account the basic structure of the 'Guideline on Security Measures under the EECC 4th Edition July 2021'. The protective measures apply to all obliged entities, are formulated in a technology-neutral manner and may need to be supplemented by specific safety profiles. In this respect, they form the basis for all protective measures to be implemented. The protective measures derived from the safety objectives must also be adequately taken into account in the safety concept to be drawn up. The assessment of the appropriateness of a security-conceptual protection measure is initially the responsibility of the obliged entity. This is a continuous assessment process in which strategies and measures are constantly reviewed and adapted to changing requirements.

The basic IT protection of the BSI can form a basis for achieving the security objectives and the protective measures to be taken for this purpose. Due to technical developments, the boundaries between pure IT and traditional telecommunications systems are becoming increasingly blurred and can no longer be clearly separated in some areas. Thus, basic IT protection forms the basis for securing these systems and must therefore be taken into account in the security objectives and protective measures described in this chapter. There are also other sources that can be used to achieve the safety objectives (e.g. ISO, ETSI, GSMA, 3GPP).

In addition, obliged entities shall implement the arrangements and measures set out in the Annex to the Catalogue. In the appendix to the catalogue, the classification of obligations in the different hazard potentials from Chapter 3.2 with categories (a), (b) and (c) remains.

For each security objective, specific protective measures to be taken by obliged entities to achieve the security objective are listed.

These protective measures are divided into 3 categories (a to c) with increasing complexity in view of the different risk potentials. The listed protective measures in the stages must be implemented cumulatively depending on the risk potential.

- c) Basic protective measures (normal hazard potential and higher)
- d) Extended protective measures (higher risk potential and higher)

e) Further extended protective measures (increased risk potential)

The background to this differentiation is the great heterogeneity of the telecommunications sector. In order to meet the wide range and the resulting risk potential of business models (large incumbent telecommunications companies, small service providers, fibre operators, mobile virtual network operators, internet access service providers, etc.), this multi-level was chosen.

Due to the technology-neutral approach, the protective measures listed here should be applicable to a wide range of different technologies. This is complemented by more detailed guidelines for certain networks and technologies, such as mobile communications.

This catalogue sets out safety objectives and the obliged entity must demonstrate that the measures it takes fully achieve the respective safety objective.

The list of protective measures is not exhaustive, but serves as a minimum requirement in the various categories of hazard potentials and serves as a guide for the obliged entity to achieve the safety objectives.

If divergent measures are implemented to achieve the safety objective, the obliged entity shall explain how it achieves the required safety objectives.

In addition, protective measures are possible and may also be necessary in accordance with the outcome of the hazard analysis. Therefore, an obliged entity with a normal risk potential may also apply extended protective measures of the higher risk potential to achieve the safety objectives. For all protective measures, the state of the art must be taken into account.

Measures should take into account the state of the art and ensure a level of security of network and information systems commensurate with the existing risk, taking into account relevant European and international standards and implementation costs. The extent of the risk exposure and the size of the operator or provider and the likelihood and severity of incidents, as well as their social and economic impact, shall be taken into account when assessing whether measures are proportionate to the risk involved.

In accordance with the principle of proportionality, all State measures must serve a legitimate purpose. They must be suitable for achieving or promoting the aim pursued (suitability). The measures must be necessary to achieve the objective (necessity) and must not be disproportionate to the objective and purpose (adequacy or proportionality in the strict sense).

Note:

The concrete measures to be implemented by the obliged entity result from the respective claims starting with "protection measures". The measures listed in the corresponding proportionality principles are to be understood only as examples of arguments of the respective protective measures.

4.1 Protection of telecommunications secrecy and personal data

The protection of telecommunications secrecy and the protection of personal data occupy a prominent position. Therefore, anyone who provides or participates in telecommunications services must take reasonable technical precautions and other measures to protect telecommunications secrecy and personal data.

The achievement of these safety objectives applies regardless of the underlying hazard potential. In this respect, it may be necessary and appropriate for the protection of telecommunications secrecy and the protection of personal data in individual cases to implement measures with an overriding risk potential.

The technical protection of personal data undergoes a legal relocation with the application of the GDPR: the data protection obligations are generally regulated in the GDPR and the BDSG. In particular, Article 32 GDPR must be observed for the security of processing. In the telecommunications sector, on the other hand, there is an exception to the general rule. Article 95 GDPR gives priority to the provisions of the ePrivacy Directive, provided that they pursue the same objective. The TKG and TDDDG transpose the corresponding provisions of the ePrivacy Directive into German law. This also applies to § 165 TKG as a transposition of Article 4(1) and (1a) of the ePrivacy Directive. In conclusion, this means that, in order to ensure the security of services, it is not Article 32 of the GDPR, but Paragraph 165 et seq. of the TKG, and thus also the present catalogue of security requirements, that must be applied. For large parts of the processing of inventory data, on the other hand, the GDPR is the relevant legal basis.

4.2 Corporate Governance and Risk Management

The area of "Management and Risk Management" includes the security objectives related to the management of network and information security risks.

Legitimate Purpose and Appropriateness

These regulations serve the legitimate purpose of ensuring the security of networks and services at all times and to identify security risks at an early stage in order to avert them accordingly. They are also suitable for this.

Necessity

The measures contained in this chapter are necessary as their objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to record an overriding safety concept in writing and at least to inform the personnel in key positions in advance. If the company were to react appropriately only when specific risk situations occurred, greater risks in particular could occur more easily. Rather, these must be taken into account in the abstract and in advance so that they can be avoided or their effects minimized. The staff must also be prepared accordingly and ensure compliance with safety regulations and implementation of measures at all times.

For companies with high and increased risk potential, it is also necessary to establish detailed network and information security guidelines and to inform the staff about the relevant security guidelines in their respective environment / area of responsibility. This ensures that the company remains capable of acting even in the event of a failure of the key personnel and if necessary. Personnel in a security role shall be formally assigned to security functions; risk management shall be regularly reviewed, as the occurrence of hazards may have an impact on the public interest.

For companies with increased risk potential, in order to be able to use industry-wide knowledge from security, the experience of own incidents and those of other providers must be taken into account when reviewing the network and information guidelines. It is not sufficient to inform the staff only; on the contrary, a special crisis unit must be set up and a 24/7 contact person must be appointed in the event of a crisis, in order to ensure a faster response time if necessary. Regular inspections and a secure traceability of the supply chain in security-related aspects must be fully guaranteed, as the occurrence of hazards can have a serious impact on the common good. This is a regulation that is also in the self-interest of the companies, since even a security-threatening behavior in the supply chain can lead to the fact that the company must be attributed this behavior according to § 278 of the German Civil Code (BGB).

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

By graduating the depth of intervention in the design of the security objectives, this balance of interests was taken into account between the legitimate purpose and the interests of the obliged entities. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the increased or higher risk potential posed by undertakings in categories b) and c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

4.2.1 Information security policy

Network and information security policies and topic-specific policies must be defined, published internally, communicated to and recognised by relevant personnel.

Safeguard measures:

a)

- Define an overarching security strategy for the security of networks and services
- Information to key personnel on the security strategy
- Review of security strategy after incidents

b)

- Establish detailed information security policies for facilities and business processes necessary to maintain networks and services
- Information to staff on security policy and its impact on the work area
- Regular check according to the hazard analysis
- Assess results of tests/exercises within the organisation in relation to information security policy

c)

- Regular review according to the risk analysis of information security policies, taking into account breaches, exceptions, past incidents and previous tests/exercises affecting other (similar) operators/providers in the industry

4.2.2 Risk management

Each obliged entity shall ensure that a procedure is established, implemented and maintained to identify risks to the security of networks, services and the processing of data worthy of protection. For this purpose, the hazard analysis can be used, among other things.

Safeguard measures:

a)

- Establishment of a list of risks to the security of networks and services, taking into account the risks to all areas
- Inform key personnel about key risks and how to mitigate them
- Review of risk assessments following changes or incidents

b)

- Establish a risk management methodology and/or tool based on industry standards
- Ensuring that key personnel apply risk management methods and tools
- Ensuring that residual risks are acceptable and accepted and lived by management
- Regular review of risk assessments
- Regular review of risk management methodologies and/or -tools taking into account changes and past incidents
- Risk analysis and security concepts for information systems

c)

- No additional measures are obligatory for this point

4.2.3 Safety Roles and Responsibilities

Personnel responsibility for the security of information, business processes, applications, tasks and regulations must be defined (e.g. information security officer, data protection officer, security officer in accordance with the TKG).

Safeguard measures:

a)

- Assignment and regular review of security roles with the appropriate competences and powers and definition of responsibilities for staff
- Ensuring that those responsible with the appropriate security role or their representatives can be reached in the event of an incident
- Inform staff about the security functions (e.g. guards and security forces) in their respective organisation and when and who to contact

b)

- Personnel in a security role are formally assigned to security functions
- Regular review of the structure of the security roles and responsibilities also with regard to changes and/or revision needs due to past incidents

c)

- Establishment of a crisis unit and a crisis/situation centre in the event of a crisis and appointment of a contact person available 24/7 in the event of a crisis
- Establishment and regular review of a process for certificates of products, if there are legal requirements for product certification

4.2.4 Security for dependencies on third parties

The provision of telecommunications networks and services can often only be made using third parties (e.g. pre-service providers, cloud providers, collocation). It is therefore necessary to ensure the introduction and maintenance of security objectives for contracts with third parties, so that dependencies on third parties do not compromise the security of networks and/or services. In such cases, security objectives and security standards that apply to the obligated company are also obligatory and contractually guaranteed for third parties. This includes contracts with energy service providers to ensure energy supply.

Note:

Providers of telecommunications services of the 5. Mobile communications generation is obliged to contractually ensure that the requirements of Chapter 5 for 5G network operators are implemented by their pre-service providers and contractual partners.

Safeguard measures:

a)

- Inclusion of safeguards in contracts with third parties, including confidentiality and secure transmission of information
- occasional review and update of third party security policies, taking into account past incidents, changes, etc.
- Overview of contracts with third parties must be available

b)

- Establishing security policies for contracts with third parties
- Ensuring integrity in all procurements of services/products

- Ensuring compliance with the guidelines by third parties
- Requirement of specific safety standards in third party processes
- Mitigation of residual risks not treated by the third party
- Creation and use of contract management for contracts with third parties

c)

- Supply chain security, including security-related aspects of the relationship between each entity and its immediate suppliers, shall be ensured.
- Tracking and documentation of incidents related to or caused by third parties
- Regular review and update of third party security policies, taking into account past incidents, changes, etc.

4.3 Security in Human Resources Management

Staff make a significant contribution to meeting the safety objectives mentioned above. Elaborate protective measures and technical redundancy concepts only bring the desired success, even if the personnel themselves do not represent a security gap in the company and are aware of the responsibility of their security-relevant activity. This chapter covers the protective measures for the human resources department, the management and the personnel in the company. This also includes personnel, which is provided externally for the execution of certain tasks.

Legitimate purpose

Legitimate purpose is to ensure security in human resources management.

Appropriateness

The verification of the reliability of personnel, as well as the provision of comprehensive training on technical safety issues, are together with the establishment of procedures, to deal with personnel changes and personnel violations, according to the respective risk potential, appropriate means to avoid risks to safety caused by personnel.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means. For companies with normal and high risk potential, it is necessary to check at least the key personnel, for companies with increased risk potential, the background check must also cover contractors and third-party providers. This results from the central role of companies with an increased risk potential for the functioning of the telecommunications infrastructure.

In order to ensure that all personnel have all the necessary security knowledge, the key personnel must be provided with appropriate training material. For companies with high and increased risk potential, regular training on safety issues is provided so that all personnel have the current safety knowledge at all times in order to avoid safety-critical situations as far as possible and to be able to act accordingly in the event of a risk.

In order to deal with personnel changes, appropriate procedures must be established in advance to avoid that only short-term security gaps arise in the event of a change of staff, for example by not withdrawing access rights or ID cards in good time.

In order to ensure that the personnel also implements the acquired security knowledge accordingly, a procedure must be established for the personnel who have violated security guidelines. For companies with higher risk potential, the remedial measures taken must also be documented and the procedure must be regularly reviewed and updated. This is the only way to react adequately to changes and incidents.

adequacy

The envisaged measures are appropriate as the intended purpose is not disproportionate to the seriousness of the interference. In accordance with the respective risk potential, it was taken into account that for smaller companies the reliability test is to be limited only to the key personnel. The key personnel must be provided with training material on safety issues, and regular safety training is required only from the heightened risk potential. It should also be noted that the training courses may also be provided by external service providers, i.e. they do not necessarily have to be designed separately for each company. The handling of personnel changes (withdrawal of access rights) must also be implemented regularly for data protection reasons.

4.3.1 Human resources management

Appropriate verification of the trustworthiness, independence and integrity of staff shall be carried out, depending on their role and responsibility.

Safeguard measures:

a)

- Verification of professional references of key personnel (system administrators, security officers, security guards, etc.)

b)

- carry out checks on key personnel, where necessary;
- Establishment of policies and procedures for staff verifications
- Review and update of measures/procedures for
Background checks and reference checks at regular intervals, taking into account changes and past incidents

c)

- Apply background checks also to contractors and third parties

4.3.2 Safety knowledge, safety training and testing

Staff must have appropriate and relevant security knowledge, develop awareness of how to handle sensitive data and undergo regular security training.

Safeguard measures:

a)

- Provide key personnel with relevant security training material

b)

- Implement a training programme to ensure that key personnel have sufficient and up-to-date security knowledge
- Organise network and service security training and staff awareness events on security issues of importance to the company
- Review and update the training programme at regular intervals
Intervals taking into account changes and past incidents
- Regular review of staff security knowledge
- Update training programmes and cover state-of-the-art innovations
- Regularly check the professional staff for the current training and qualification carried out before the staff gains access to safety-critical areas

c)

- No additional measures are obligatory for this point

4.3.3 Personnel changes

Introduce and maintain an appropriate procedure for dealing with personnel changes or changes in their roles and responsibilities.

Safeguard measures:

a)

- After personnel changes, access rights, badges, equipment, etc. are immediately withdrawn if they are no longer required or permitted, corresponding evidence must be kept
- Instructing and training new staff in the applicable policies and procedures

b)

- Establishment of a staff transfer procedure, taking into account the timely withdrawal of access rights, badges, equipment, etc.
- Implementation of measures/procedures for the training of staff in new roles
- Regular review of the effectiveness of procedures

c)

- Documentation of improvement possibilities and direct application, if possible

- Review, evaluation and adaptation of measures/procedures for personnel changes taking into account changes and past incidents

4.3.4 Dealing with infringements

Introduce and maintain a procedure for personnel who have violated security policies. A comprehensive procedure should be in place to detect incidents caused by staff violations.

Safeguard measures:

a)

- Establishment of a procedure that detects violations of directives and takes appropriate countermeasures

b)

- Establishment of procedures in the event of staff non-compliance with the guidelines and documentation of remedial actions taken
- Regular review and update of the procedure based on changes and past incidents

c)

- No additional measures are obligatory for this point

4.4 Security of data, systems and facilities

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

Legitimate purpose

These points serve to ensure the physical and logical security of data, network and information systems.

Appropriateness

The establishment and maintenance of physical and logical safeguards to prevent unauthorised access is likely to promote the security of networks, information systems and facilities. Measures to protect the equipment from power outages and other disturbances are appropriate means to promote security of supply. Unique identifiers and access control mechanisms are appropriate means to prevent unauthorized use of devices and systems, disclosure of confidential information and malfunctions, and to prevent tampering. The implementation of protection measures against attack vectors such as viruses, code injections or malware are suitable to promote the integrity and availability of network and information systems. Encryption algorithms are suitable to protect the networks and systems against unauthorized access.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to take measures to prevent unauthorised physical and logical access to facilities and infrastructure. In order to protect access, companies with high and increased risk potential must also develop strategies that must be regularly monitored and reviewed. Companies with increased risk potential must regularly update these strategies in order to be able to react to current risks at an early stage and also to ensure a fail-safe remote shutdown or data deletion for stolen devices.

In order to ensure security of supply, devices and equipment must be protected against power outages and other malfunctions. With regard to the failure of the public electricity grid, companies with high risk potential must define which critical areas of the operation must be maintained in order to protect necessary supplies in advance. Companies with increased risk potential also need to have active cooling and emergency generators in place to ensure supply is secured.

The implementation of logical access control mechanisms is a suitable means to prevent unauthorized use of devices and systems. Unauthorized access can only be prevented by using unique identifiers of users and systems. Companies with high risk potential must monitor access to network and information systems. Companies with increased vulnerability also need to assess the effectiveness of their access control policies and procedures, and their authentication mechanisms need to be in line with general best practices, such as: Multifactor Authentication (MFA).

In order to protect the integrity and availability of network and information systems, companies with normal risk potential must ensure, for example through input controls and firewalls, that attack vectors using viruses or malware cannot be used to access the systems. For companies with high risk potential, this requires increased controls on software integrity in order to ward off attack vectors in advance. Companies with increased risk potential must use software patching procedures to ensure that software products receive security-relevant patches as quickly as possible.

Encryption shall be used to secure against unauthorised access. Companies with higher risk potential must introduce and implement encryption policies and algorithms to ensure a standardized procedure, while companies with higher risk potential must regularly review and update these policies to ensure the current state of the art.

Security-relevant data must be protected using encryption and authentication measures. Companies with high and increased risk potential must implement special procedures for this, which must be regularly reviewed and updated.

adequacy

The measures are appropriate as the intended purpose is not disproportionate to the seriousness of the interference. According to the respective risk potential, it was taken into account that smaller companies must also take appropriate protective measures to ensure the security of data, systems and facilities, but companies with higher and increased risk potential must provide more comprehensive strategies and procedures for this purpose. Companies with increased risk potential must also regularly review, document and update their strategies. In doing so, they must take into account generally applicable standards and guidelines in order to achieve the best possible level of protection according to the state of the art (for the term 'state of the art', see above in the general comments on proportionality). In contrast to other points, point 4.4 contains requirements for companies, some of which require significant investments in terms of both financial and human resources. This results from the fact that data security includes both the physical and logical security of data, network and information systems. In order to ensure the comprehensive protection of data, it is not enough to establish only protection against physical destruction; on the contrary, protection against manipulation must also be provided for in order to ensure the security of networks and services. cf. § 3 No 52 TKG. "Security of networks and services" means the ability of telecommunications networks and services to defend against, at a certain level of confidence, all attacks that affect the availability, authenticity, integrity or confidentiality of those networks and services, of the stored, transmitted or processed data or of the related services offered or accessible through those telecommunications networks or services.

Since the different risk potentials also require different levels of trust, this already results in the different depth of intervention for the companies classified differently.

4.4.1 Physical and environmental security

Establish and maintain adequate physical and environmental security of networks, information systems and facilities.

Safeguard measures:

a)

- Prevention of unauthorised access and access to facilities and infrastructure
- Setting up appropriate environmental controls (e.g. cameras, sensors, alarms) to protect against unauthorised access/access, burglary, fire, flooding, etc.

b)

- implementing a physical protection strategy; and
Environmental controls (e.g. measures of physical protection, including the installation of fences and barriers, instruments and procedures for monitoring the environment, i.e. the use of detection devices)
- Implementation of access and access controls
- Increased access controls and access to safety-critical areas
- Verification of the effectiveness of access and access controls
- Regular evaluation of the effectiveness of access and access controls

c)

- Review and update the physical protection and environmental control strategy, taking into account changes and past incidents
- Documentation of additional, risk-based physical security controls
- Documentation of additional, adequate physical infrastructure controls (e.g. security of infrastructure and administrative buildings, alarms and video surveillance to detect and record incidents), in particular for unmanned installation sites
- Establish controls that enable fail-safe remote shutdown (or data erasure) of stolen devices and/or require re-authentication or configuration following a physical attack or power outage
- maintaining evidence of access controls, that persons entering premises are security screened, trained and qualified, and that any access, in particular by third parties, is monitored;

Note:

Under "unmanned plant locations" are e.g. POP locations, landing stations, mobile phone technology locations of high relevance and Far-Edge-RZ to be understood

Basically, antenna locations fall under the phrase "unmanned plant locations". However, they can be excluded if only a negligible risk due to e.g. theft, manipulation or sabotage is detected in the context of the hazard analysis.

4.4.2 Security of supply (availability of the entire system)

Appliances and equipment shall be protected against power outages and other disturbances caused by supply failures.

Safeguard measures:

a)

- Ensuring relevant supplies to ensure security of supply

b)

- With regard to the failure of the public electricity grid, it is necessary to define the extent to which operation or individual particularly critical areas must be maintained.
- Implement a concept for securing key supplies to ensure security of supply
- Implementation of protective measures to protect necessary supplies and supporting equipment (e.g. passive cooling, automatic restart after a power cut, emergency batteries, diesel generators, replacement fuel, etc.)
- Regular review and update of measures and procedures to secure important goods and ensure security of supply, taking into account changes and past incidents as well as the state of the art of energy storage facilities

Note:

With regard to emergency power supply, the guideline 'Emergency power supply in companies and authorities' of the Federal Office for Civil Protection and Disaster Assistance must be taken into account

c)

- Introduction of measures to protect necessary supplies (e.g. active cooling, emergency generators, service level agreement (SLAs) with fuel suppliers, redundant cooling and power supply systems)

4.4.3 Access and access control to network and information systems

Unauthorized use of devices and systems cannot be prevented without appropriate access and access control mechanisms. Unauthorized persons can also obtain confidential information, carry out manipulations or cause disturbances. Appropriate authorisations must be used to control and control access to network and information systems.

Safeguard measures:

a)

- Users and systems have unique identifiers and are authenticated before accessing services or systems
- Implementation of logical access control mechanisms for network and information systems to allow only authorised use
- Passwords are at least hashed and, if technically possible, stored with a salt
- Implement measures to protect access to network and information systems, such as roles, rights, responsibilities and procedures, for the allocation and withdrawal of access rights
- Depending on the type of access, sufficiently secure authentication mechanisms must be used, e.g. multi-factor authentication
- Regular review of granted roles and rights
- Ensuring that access by third parties and/or remote access to operational and security-related systems is granted only for the required period of time and that no permanent access data is granted

b)

- Monitoring access to network and information systems
- Establishing a procedure for granting exemptions and registering breaches of access
- Regular checks for remote access to operational network and information systems by third parties

c)

- Assessing the effectiveness of access control policies and procedures and carrying out cross-checks of access control mechanisms
- Access control procedures and mechanisms need to be reviewed and, if necessary, revised without delay
- Implemented authentication mechanisms must comply with the general best practices for multifactor authentication (MFA)
- Central solution for Privileged Access Management (PAM)

4.4.4 Integrity and availability of network and information systems

The integrity and availability of network and information systems and the protection against attack vectors by means of viruses, code injections, malware, etc., which can change the functionality of systems, must be guaranteed.

Safeguard measures:

a)

- Ensure that the software of network and information systems is not tampered with or altered, e.g. through the use of input controls and firewalls
- Continuous checks for malware in (internal) network and information systems
- Securing servers against misuse, e.g. by deactivating unneeded services

b)

- Implementation of protective measures that provide comprehensive protection against manipulation and changes to systems and ensure the availability of networks and systems
- Regular increased controls on software integrity, update and patch management for operationally relevant areas in networks
- Provide sufficient redundancies to ensure the availability of operationally relevant systems

c)

- Establishing effective controls to protect the integrity of systems
- Assessing and reviewing the effectiveness of measures to protect the integrity of systems
- Use secure software patching procedures to ensure that software products or components have been modified only in the desired way (e.g. appropriate cryptographic methods to protect integrity and authenticity)

4.4.5 Ensuring confidentiality

In particular, measures shall be taken to prevent unauthorised access in order to secure telecommunications and data processing systems and to minimise the impact of incidents on users and other telecommunications networks and services.

Safeguard measures:

a)

- When transmitting and storing data, confidentiality, the protection of telecommunications secrecy and the protection of personal data must be adequately ensured by encryption or access by third parties must be securely excluded by other measures
- In the case of planned new acquisitions, replacement of telecommunications and data processing systems or restructuring, measures for encryption should be adequately taken into account in the planning and implementation
- Where mobile device software ('app') is made available to customers as part of the service, the data stored on the device and transmitted shall be encrypted.

Note: Further information on the state of the art of encryption can be found in the TR-02102.

b)

- Introduction and implementation of an encryption policy
- Use of encryption algorithms taking into account the recommended minimum length of the cryptographic key used
- Occasional review and update of the encryption policy
- For systems offering a choice of different levels of security, the highest possible level of security should be used
- Concepts and procedures for the use of cryptography and encryption

c)

- Regular review and update of encryption policy

4.4.6 Protection of security-related data

Ensure that cryptographic key material and secret authentication information are adequately protected.

Safeguard measures:

a)

- Ensuring that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) cannot be disclosed or manipulated
- Strict control and monitoring of access to private cryptographic keys

b)

- Implementation of procedures for the management of cryptographic keys
- Implementation of a password management procedure
- Regular review and update of the key management policy
- Regularly review and update the password management policy
- Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and, where applicable, secured emergency communication systems within the facility

c)

- No additional measures are obligatory for this point

4.5 Operational management

Responsible corporate governance shall ensure proper and safe operation. The following protective measures concern the operational process, change management and the handling of corporate values.

Legitimate purpose

Legitimate purpose is to ensure proper and safe operation.

Appropriateness

The definition and implementation of operational procedures, predefined methods or procedures for changes to operationally relevant systems as well as asset management procedures and configuration controls are appropriate means to ensure proper and safe operation.

Necessity

The measures are necessary as their objective cannot be achieved by any other equally effective means. For undertakings with normal risk potential, it is necessary to establish operational procedures and the allocation of responsibilities for the operation of key systems. Companies with higher and higher risk potential must implement strategies and regularly review and update them to ensure that all important systems are operated and managed. Only by defining such strategies in advance can it be guaranteed that networks and services will be maintained at all times. Companies with a higher risk potential must also put in place mechanisms to ensure that every actual change is recorded and that any irregularities are investigated.

To avoid disruptions or incidents, changes to network and information systems, infrastructures, documentation, processes, procedures and operations must be planned, controlled and controlled using predefined methods or procedures. If the procedure were only defined at the same time as the change occurring, there would be a risk that hasty or unsuitable change management would lead to security risks. Companies with higher and higher risk potential must define predefined change management procedures, document them, regularly review and update them, and set up and use a patch management system. For organizations with increased risk potential, changes to the virtualized network environment must also be included in change management policies and procedures.

In order to manage the availability of important assets and configurations of critical network and information systems, an asset management procedure and configuration controls must be established. Important plants must be identified and documented in advance. Important systems and those containing personal data must be configured and protected. Companies with high and increased risk potential must implement, review and update appropriate procedures. Companies with increased risk potential must additionally use data storage with the relevant details and about the technologies and components used.

adequacy

These measures are appropriate as the intended purpose is not disproportionate to the seriousness of the interference. In determining the measures to be established, the respective risk potential was taken into account. Companies in category (a) must establish safe operating procedures and change management. Companies with high and increased risk potential need to establish more comprehensive procedures. In addition, companies with increased risk potential must introduce even more comprehensive mechanisms, regularly monitor them and keep them up-to-date with the latest technology at all times.

4.5.1 Operational procedures

Appropriate operational procedures shall ensure that all relevant operations of the relevant obliged entity function properly, safely and continuously.

Safeguard measures:

a)

- Establishment of operational procedures and allocation of responsibilities for the operation of key systems

b)

- Implement a system operation strategy to ensure that all key systems are operated and managed in accordance with predefined procedures
- Regular review and update of the measures/procedures for the operation of the systems necessary for the maintenance of networks and services, taking into account incidents and/or changes

c)

- Introduce mechanisms to ensure that every actual change is recorded and that any irregularities that occur during the change process are investigated

4.5.2 Change management

In order to avoid disruptions or incidents, changes to network and information systems, infrastructures, documentation, processes, procedures and operations must be planned, controlled and controlled and reviewed after completion.

Safeguard measures:

a)

- Compliance with predefined methods or procedures when making changes to operationally relevant systems

- Apply security patches within a reasonable period of time upon their availability, verify their trusted origin and integrity

b)

- Implement change management measures/procedures to ensure that changes to operationally relevant systems are always made following a predefined procedure
- Documentation of change management procedures and record of all changes to the procedure
- Regular review and update of the change management process, taking into account changes and past incidents
- Setting up and using a patch management system
- Implement overarching security measures in the acquisition, development and maintenance of network and information systems, including vulnerability management and disclosure

c)

- Changes to the virtualized network environment (e.g. by patching software-defined network components) must be included in the change management policies and procedures

4.5.3 Asset Management

Establish and maintain asset management procedures and configuration controls to manage the availability of critical assets and configurations of critical network and information systems.

Safeguard measures:

a)

- Identification and documentation of important installations and configurations of important systems as well as systems containing personal data
- Documentation of the systems that are connected to the aforementioned systems and could be misused for attacks, e.g. in the form of a network structure plan

b)

- Implementation of measures/procedures for asset management and configuration control
- Regular review and update of asset management based on changes and past incidents

- Creation of an overview of the dependencies of important plants, configurations of important systems and important / critical software

c)

- Establish and regularly update documentation detailing the technologies and components used
- Carrying out regular assessments of physical assets by introducing strategies/procedures in asset management
- Categorisation of physical network facilities (e.g. core network facilities, transmission nodes, switching points, base stations) based on risk analysis and in relation to the importance of operationally relevant systems

4.6 Lifecycle management for hardware and software

Since products are exposed to different risks during their life cycle in the respective phases, these risks must be minimised. For particularly critical phases, the following requirements are therefore imposed on the obliged entity, but also on the functional scope of the components. Lifecycle management is used to ensure the integrity of the hardware and software used.

Legitimate purpose

The legitimate purpose is to minimize the security risks that can arise in the various life cycles of hardware and software.

Appropriateness

The definition and implementation of measures, according to the respective risk potentials, for the duration of the use and the exchange process of components is an appropriate means to minimize the security risks in the various life cycles of hardware and software.

The exchange of components that are no longer up-to-date and the integrity check binds financial and human resources, serves both the legitimate purpose of minimizing the risk potential in all categories.

Necessity

The measures are necessary as their objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to replace the components after the end of support, as safe operation can no longer be guaranteed after this period. Companies with high risk potential must be able to verify the integrity of the purchased products at all times. This is the only way to ensure that the components have not been tampered with during delivery. Companies with increased risk potential must provide hardware products with physical protection such as seals upon delivery so that effects on the product are immediately recognizable externally. When decommissioning, further requirements must be met and sensitive data must be permanently deleted so that it cannot be restored.

adequacy

The measures are also appropriate as the intended purpose is not disproportionate to the seriousness of the interference. This balancing of interests was taken into account by grading the depth of intervention in the design of the safety objectives. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the higher risk potential of undertakings in categories (b) and (c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

Safeguard measures:

a)

- Replacement of components, e.g. if they can no longer be operated safely after the end of the support period

b)

- The obliged entity must be able to verify the integrity of the hardware and software products purchased at any time, starting with acceptance. The examination possibilities must be used accordingly and documented.
- In particular, it shall be examined whether the components concerned have been tampered with, influenced or otherwise altered during delivery.

c)

- For hardware products, suitable physical protection must be provided upon delivery, e.g. sealed transport boxes, guarded transports or self-protection of the product (e.g. the use of cryptographic methods for integrity assurance)
- For software products, principles such as security-by-design must be taken into account and the requirements of the Cyber Resilience Act (CRA) must be observed.
- The integrity of the product must be ensured during storage.
- Once again, an integrity check must be carried out during commissioning and included in the configuration management
- When decommissioning, special requirements (e.g. secure deletion of key material, configurations, personal data, e.g. traffic data, etc.) must be taken into account.

4.7 Incident management

Incident management includes the actual management process, the ability to detect, report and cooperate on incidents across telecommunications providers.

This includes recognising, responding to and reporting disruptions and incidents. Incidents can be triggered by a single event or a chain of different circumstances. These may compromise the confidentiality, integrity, availability or authenticity of information and telecommunications systems.

Legitimate purpose

Legitimate purpose is the detection, response and reporting of disruptions and incidents to protect the confidentiality, integrity, availability and authenticity of information and systems.

Appropriateness

This interference serves the legitimate purpose of protecting the confidentiality, integrity, availability and authenticity of information and systems. The strategies mentioned are also suitable for this purpose.

The definition and implementation of comprehensive security strategies according to the respective risk potentials is an appropriate means of ensuring the protection of the confidentiality, integrity, availability and authenticity of information and systems.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to ensure human resources prepared to deal with incidents and to set up processes to detect incidents. Communication and reporting to third parties, customers and authorities may be necessary to prevent similar incidents in the future.

The addressees of the intervention must provide human resources and – if there is a high and increased risk potential – also establish appropriate processes. There are no other equally effective means of protecting information and systems equally from incidents. In particular, the transparent handling of incidents serves to prevent similar incidents in the future.

Companies with high risk potential must establish industry-standard systems and procedures for incident management in order to be fully prepared. This includes procedures for communicating and reporting incidents. In cases of disruptions that could affect several operators / providers, contact persons and procedures must be coordinated in advance so that direct and immediate contact is possible in an emergency in order to be able to react as quickly and adequately as possible to hazardous situations.

In addition, companies with an increased risk potential must also take into account the findings of previous incidents when assessing their procedures for managing their incidents, in order to include the information obtained from them and to monitor all safety-related network activities.

adequacy

The measure is proportionate as the intended purpose is not disproportionate to the seriousness of the interference. This balancing of interests was taken into account by grading the depth of intervention in the design of the safety objectives. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the higher risk potential of undertakings in categories (b) and (c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

The balancing of interests took into account that the detection of IT security gaps is in the self-interest of the respective addressee.

Against this background, the requirements are partly obligations, i.e. behavioural requirements in their own interest. The depth of intervention has been designed in such a way that very small companies in particular do not have to introduce separate processes. Against this background, the above measures are overall proportionate.

4.7.1 Incident management procedures

Establish, maintain and update procedures to deal with incidents and forward them to appropriate personnel.

Safeguard measures:

a)

- Ensuring human resources prepared to deal with incidents
- Keeping records of all major incidents
- Case-by-case investigation of incidents and measures taken

b)

- Implementation of incident management measures/procedures
- Investigation of major incidents and preparation of final reports, including measures taken and recommendations to avoid future incidents of this nature

c)

- Assessment of principles/procedures for incident management based on previous incidents

4.7.2 Ability to detect incidents

Establish and maintain an incident detection system.

Safeguard measures:

a)

- Establishment of incident detection processes
- Possibility of contact for receiving external messages

b)

- Implementation of industry-standard systems and procedures for incident detection
- Introduce systems and procedures for recording and timely reporting of incidents to competent bodies
- Regular review of incident detection systems and procedures and their update taking into account changes and past incidents
- Periodic review of relevant protocols following predefined procedures related to remote access to the network
- Incident management approaches

c)

- Introduce incident detection systems and procedures
- Monitoring of safety-related network activities

4.7.3 Incident reporting and communication

Establish, maintain and update incident reporting procedures.

Safeguard measures:

a)

- Communicate and report on ongoing or past incidents to third parties, customers and/or authorities, if necessary

b)

- Implementation of measures and procedures for communication and reporting on incidents

- Regular review and update of reporting and communication plans based on changes or past incidents

c)

- Assessment of the procedure based on previous notifications and incident reports

Note:

There are different types of incidents for which the obliged entity must put in place appropriate and appropriate procedures.

Should there be a significant impact on the operation of the networks or on the provision of the services in the event of an incident, this shall be classified as a security incident pursuant to § 168 TKG and shall be notified immediately to the BNetzA and the BSI.

Further information on security incidents pursuant to § 168 TKG can be found on the BNetzA website [at www.bundesnetzagentur.de/security incident](https://www.bundesnetzagentur.de/security%20incident) .

In addition, providers of publicly accessible telecommunications services are obliged to notify the Federal Network Agency and the BfDI immediately in the event of a personal data breach (§169(1) TKG).

4.7.4 Cooperation in telecommunications provider-independent disruptions

If disruptions occur that could affect several operators/providers, for example due to DDoS attacks, an overarching cooperation between operators/providers is necessary. This should include an overarching exchange of operators/providers on infected devices.

Safeguard measures:

a)

- Basic protective measures to achieve the safety objective

b)

- Contact persons and procedures should be coordinated with each other in advance. This also includes the designation of an Abuse contact that is responsive at least during office working hours, through which incoming messages are processed (if necessary automatically).
- It is the responsibility of the obliged entity to contact networked operators/providers to identify the appropriate contact persons. In return, the latter must inform the first operator/provider immediately of any changes.
- It must be ensured that direct and immediate contact between operators/providers is possible in the event of an emergency.

- In the event of a crisis, a contact option must be published on the Internet.

c)

- No additional measures are obligatory for this point

4.8 Emergency and failure management

A malfunction or incident may lead to the failure of the service or network operation. An appropriate prevention strategy should take into account such developments and develop appropriate defence concepts adapted to the individual case. Contingency and failure management includes continuity strategies and contingency plans to prevent or mitigate major failures and natural or man-made disasters.

Note:

A procedure for the systematic development of comprehensive emergency and failure management is²⁹ described in the BSI standard 200-4.

Legitimate Purpose and Appropriateness

This point aims at preventing or mitigating major service or network failures and disasters through continuity strategies and contingency plans. The definition and implementation of comprehensive security strategies according to the respective risk potentials is an appropriate means of preventing disruptions or incidents from leading to the failure of the service or network operation.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to implement contingency plans and a strategy to ensure the maintenance of services and networks in order to prevent disruptions and incidents from leading to failure. Regular backups of all systems and data necessary for the operation of the network and/or the provision of telecommunications services shall be made. Companies with normal risk potential should only store backup data and systems spatially and logically separate from the systems of active operation; Companies with high and increased risk potential must do so. Thus, the safety catalog for companies with normal risk potential remains under the 3-2-1 rule for backups, which is generally accepted as a best practice rule.³⁰ Particularly in view of the fact that ransomware attacks have increased sharply in recent years and have also been successful to a considerable extent, a backup strategy for the security of data and the functioning of the telecommunications infrastructure in Germany is an integral part and also in the self-interest of every company. Companies with high and increased risk potential must also implement contingency plans for operationally relevant systems and processes and regularly review and revise them.

Companies with increased risk potential must also take into account the findings of previous incidents when assessing their contingency plans and take special precautions to cover time-critical applications and ensure higher network availability.

adequacy

²⁹ <https://www.bsi.bund.de/dok/531576>

³⁰ Thereafter, 3 backup copies are to be made on 2 different storage media; A backup copy should be stored off-site.

The measure is proportionate as the intended purpose is not disproportionate to the seriousness of the interference. This balancing of interests was taken into account by grading the depth of intervention in the design of the safety objectives. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the higher risk potential posed by undertakings in categories (b) and (c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

4.8.1 Strategy for maintaining networks, services and contingency plans

Establishing and maintaining contingency plans and a business continuity management strategy for operated networks and telecommunications services are essential.

Safeguard measures:

a)

- Implement a strategy to maintain the telecommunications networks and/or services provided

b)

- Implementation of contingency plans for all operationally relevant systems, processes, sectors and services
- Monitoring contingency plan activation and execution, and registering the times necessary for successful or failed recovery
- Regular review and revision of the strategy for maintaining networks and services, e.g. preparedness with sufficient redundancies

c)

- Review and revision of contingency plans based on changes and past incidents
- Provision of special precautions added to existing contingency plans to cover time-critical applications to ensure higher network availability for such services
- Creation of an overview of operational dependencies (e.g. in the context of supply chains, pre-service providers, emergency supplies, etc.), which can have a direct or indirect impact on the availability or continuity of networks/services. Corresponding remedial measures must be defined and documented. This includes, inter alia, the supply of energy through emergency measures (e.g. with mobile network replacement systems) for those network elements that are indispensable for the operation of a network or the maintenance of a service.

4.8.2 Disaster Recovery Management

The obliged entity shall establish and maintain appropriate emergency mechanisms to restore telecommunications networks and services in the event of natural disasters, sabotage and/or other disasters.

Safeguard measures:

a)

- Preparation and documentation of concrete plans for the reconstruction and restoration of services and networks after incidents. Appropriate documentation must be available immediately in the event of an emergency.
- Documentation of restart times for the central services and networks

b)

- Implementation of measures/procedures for the use of disaster recovery management, e.g. preparation of an emergency manual
- Implementation of disaster recovery management systems. Alternatively, these can also be made available by third parties (e.g. by national emergency networks).
- Regular tests to verify that the emergency measures are effective and that the restart times provided for in the documentation are met
- Regularly review and update disaster recovery capabilities, taking into account changes, past incidents, and the results of tests and exercises

c)

- Sufficiently sized disaster recovery capacities, including in terms of energy supply, to mitigate external attacks and disasters
- Plans in the event of a disaster affecting the day-to-day operation of the network and service
-

4.8.3 Backup strategy

Regular backups of all systems and data necessary for the operation of telecommunications networks or the provision of telecommunications services shall be created.

Attention must be paid to the legally prescribed deletion and storage periods, in particular the storage period of the backups should be proportionate to the storage period of the personal data.

Safeguard measures:

a)

- The backup data and systems should be stored spatially and logically separately from the systems of the active operation
- The backup media and systems shall be checked for proper functioning at reasonable intervals.
- It shall be verified at reasonable intervals that, in the event of a disruption of the effective operation of the backups, the continued uninterrupted operation of the network and telecommunications services is ensured.
- All backup procedures must be documented and this documentation must be kept with the backup data

b)

- Backup data and systems must be stored spatially and logically separate from the operating systems
- Establishment of geo-redundant backup solutions to minimise disruptions to telecommunications services due to failures of central technology sites

c)

- No further action required

4.9 Monitoring, testing and testing procedures

In order to make systems and processes as secure as possible and to optimise them at all times, monitoring, testing and testing procedures of network and information systems and facilities must be introduced.

Legitimate purpose

Legitimate purpose is the introduction of monitoring, testing and testing procedures of network and information systems and facilities in order to make systems and processes as secure as possible.

Appropriateness

The definition and implementation of comprehensive safety strategies according to the respective risk potentials is a suitable means to make systems and processes as safe as possible.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means. For companies with normal risk potential, it is necessary to identify and monitor systems and relevant interfaces required for operation. Specifications are required for testing systems when new networks or systems are connected.

Companies with elevated and increased risk potential must deploy intrusion detection systems and implement programs to regularly practice backup and emergency plans. Here is a clear leap in the requirements towards companies with normal risk potential. As a result, the setting up of corresponding tools and the associated monitoring are mentioned as independent points in the catalog. Companies with increased risk potential must implement systems for attack detection according to certain guidelines and also involve suppliers and third parties in the emergency exercises.

With regard to the contingency plans, the difference between the risk potentials is that companies with a normal risk potential only have to carry out abstract exercises, while the larger companies – which are also more attractive as targets – also have to play through concrete scenarios. Companies with increased risk potential must also involve suppliers and third parties in order to ensure the safety of the entire process chain at least fundamentally.

The purpose of testing networks and information systems before they are implemented is to ensure ongoing operation. In the past, it has been shown that this point is not only used to prevent manipulations, e.g. by malware; rather, the compatibility and behaviour of the software in the existing system can be checked before it is used in the productive system.

The protective measures must take into account the state of the art (see comments on general proportionality). They also need to adapt to the growing threat landscape. Against this background, companies with normal risk potential must ensure that regular safety tests are

carried out. Companies with higher/increased risk potential must also check the safety tests themselves and adapt them if necessary.

Compliance with and implementation of legal and regulatory requirements are as such part of a properly executed business; in this respect, the safety catalogue for companies with normal risk potential does not contain any additional requirements. The fact that companies with higher/increased risk potential must optimise monitoring, on the other hand, constitutes their own regulation, but its depth of intervention is low.

adequacy

The measure is proportionate as the intended purpose is not disproportionate to the seriousness of the interference. This balancing of interests was taken into account by grading the depth of intervention in the design of the safety objectives. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the higher risk potential of undertakings in categories (b) and (c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

4.9.1 Intrusion detection, monitoring and logging systems

In order to detect disruptions that may cause significant disruption to telecommunications networks and services and to manage risks to the security of networks and services, it is necessary to monitor all systems and networks relevant to their operation or provision. This may require the collection of log and logging data for the identification and evaluation of security-relevant events (SRE) and the use of systems for attack detection. When implementing these measures, both the data protection requirements and the requirements for telecommunications secrecy must be observed.

Safeguard measures:

a)

- Identification of systems and relevant interfaces relevant to the operation of telecommunications networks and/or the provision of telecommunications services
- Monitoring of these systems/interfaces

b)

- Recommendation on the use and operation of intrusion detection systems Details can be³¹ found in the BSI's guidance on intrusion detection systems

c)

- Deployment and operation of intrusion detection systems at least equivalent to level 4 of the BSI's Level of Implementation Model of Guidance on Intrusion Detection Systems.

³¹ <https://www.bsi.bund.de/oh-sza>

They are equivalent if, in particular, they have equal attack detection capacities and can thus ensure an equivalent level of security.

4.9.2 Emergency exercises

Safeguards to maintain and restart infrastructure and services after incidents, outages and emergencies must be in place and implemented.

It is necessary to periodically review the established and implemented safeguards and contingency plan measures, including in cooperation with third parties, to ensure that they are valid and effective in adverse situations.

Safeguard measures:

a)

- Exercise and test backup and contingency plans to ensure systems and processes are working and staff are prepared for major outages and uncertainties

b)

- Implementation of a program for the regular exercise of backup and emergency plans, using realistic scenarios
- Ensure that lessons learned from the exercises are taken up by those responsible and that the relevant processes and systems are updated accordingly.
- Regular review and update of exercise schedules taking into account changes, past events and incidents not included in the exercise programme

c)

- Involvement of suppliers and other third parties in the exercises, e.g. business partners and customers
- Participate in tests/exercises with other (similar) operators/providers in the industry

4.9.3 Testing of network and information systems

Changes or development work on existing network and information systems are possible risk factors. It is therefore necessary to lay down rules for testing network and information systems, in particular when new networks or systems are connected.

Safeguard measures:

a)

- Testing of network and information systems before they are introduced or connected to existing systems

b)

- Implementation of measures/procedures for testing network and information systems
- Implementation of tools for automated testing
- Regular review and update of measures/procedures for testing, taking into account changes and past incidents

c)

- No additional measures are obligatory for this point

4.9.4 Assessment of protective measures

The protection measures must take into account the state of the art and thus adapt to the growing threat situation. Against this background, it is necessary to define and maintain an appropriate strategy for carrying out security assessments of network and information systems.

Safeguard measures:

a)

- Ensure that key systems are subject to regular security reviews and security tests, in particular when introducing new systems and following changes

b)

- Implementation of measures/procedures for safety assessments and safety tests
- Regular review and update of measures/procedures for safety assessments and safety tests, taking into account changes and past incidents
- Concepts and procedures for assessing the effectiveness of measures in the field of security of networks and services, based on a cross-hazard approach aimed at protecting network and information systems and the physical environment of these systems from incidents

c)

- Assessing the effectiveness of protective measures and safety procedures
- Assessment of safety tests

4.9.5 Compliance monitoring

Introduce and implement procedures to monitor compliance with standards and legal regulations.

Safeguard measures:

a)

- Monitoring compliance with and implementation of legal requirements

b)

- Continuous monitoring of compliance with standards and legal requirements
- Regular review and update of compliance and audit measures/procedures, taking into account changes and past incidents

c)

- Assessment of compliance and verification measures/procedures

4.10 Threat Awareness

This area includes security objectives related to threat intelligence and contact with end-users to share information on key threats to the security of networks and services.

Legitimate purpose

Awareness of threats includes information about threats and informing users about threats. This serves to obtain information on the main threats to the security of networks and services and to share them with end customers by defining and implementing comprehensive security strategies. These are also adapted to the respective risk potentials.

Appropriateness

The definition and implementation of comprehensive security strategies according to the respective risk potentials is an appropriate means to achieve the security of networks and services.

Necessity

The measure is necessary because its objective cannot be achieved by any other equally effective means.

It is necessary for companies with normal threat potential to carry out threat analysis programmes and to inform end-users of networks and services about security threats in the context of education.

Companies with higher and higher risk potential must implement appropriate programmes and measures to inform users about security threats on a regular basis; Companies with increased risk potential must also regularly review and update these measures.

adequacy

The measure is an information mechanism that is neither financially nor humanly inappropriate. In particular, the measures are also adapted to the respective risk potentials. The measure is proportionate as the intended purpose is not disproportionate to the seriousness of the interference. This balancing of interests was taken into account by grading the depth of intervention in the design of the safety objectives. Companies in category (a) only need to implement less restrictive measures to achieve the safety objective. In view of the higher risk potential of undertakings in categories (b) and (c) to ensure the security of networks and services, it is also reasonable for those undertakings to have a more serious interference with their freedom to choose an occupation.

4.10.1 Threat Intelligence

Establish and maintain appropriate mechanisms to monitor and gather information on relevant threats to the security of networks and services.

Safeguard measures:

a)

- Conducting a regular threat analysis

b)

- Implementation of a threat intelligence and analysis process (e.g. threat analysis software)
- Regular review and update of the implemented threat analysis process

c)

- No additional measures are obligatory for this point

4.10.2 Informing users about threats

Users shall be informed of specific and significant security threats to the network or service that may affect users. Users must be informed of measures they can take to protect the security of their communications.

safeguards

a)

- inform users of telecommunications networks and services of specific and significant security threats to the network or service that may affect them and of possible remedial measures;

b)

- Implement measures/procedures to regularly inform users about security threats to the network or service that may affect them

c)

- Regular review and update of measures/procedures to regularly inform users of security threats to the network or service that may affect them

5. Defining additional details and measures for 5G networks

The following Chapter 5 is addressed to operators of public mobile networks of the 5. Generation ('5G network'). '5G network' in the context of the catalogue is the set of all network infrastructure elements and technologies enabling the implementation and implementation of the 5G standard,³² including the respective modes of operation (see below) in the context of European 5G harmonisation. The implementation of the 5G standard is subject to legally binding harmonisation and regulatory decisions.

For 5G networks, architecture options are defined³³ for the 5G non-standalone (5G NSA) and 5G standalone (5G SA) operating modes, which form the network or subnets individually, side by side or dynamically configurable.

In addition to the radio access networks specified by the 3GPP, other access networks (Non-3GPP Access and Open-RAN) can be integrated³⁴ into a 5G network and thus become part of the 5G network in the context of the catalogue. Insofar as these access networks or components thereof are provided by the 5G network operator, the provisions of the catalogue of security requirements shall apply mutatis mutandis to these access networks or the corresponding components.

5.1 Determination of critical components

Components that partially or fully implement the critical functions defined below must be identified and documented as critical components in the security concept.

Critical components within the meaning of § 2 No 23 BStG may only be used by an operator of public telecommunications networks with an increased risk potential if they have been checked and certified by a recognised certification body before being used for the first time (§ 165(4) TKG).

The list of critical functions is set out in Annex 2.

³² 3GPP Release 15 ff.

³³ In the 3GPP standardisation and the GSMA, these options are referred to as 1, 2, 3, 3a, 3x, 4, 4a, 5, 6, 7, 7a, 7x, 8 and 8a and can be found in 3GPP RP-161266, 5G architecture options – full set, Joint RAN/SA meeting, 14.06.2016 and 3GPP TR 38.801.

³⁴ For non-3GPP access (trusted, untrusted, wireline) see e.g. ETSI TS 123 501 and ETSI TS 123 401/402

5.2 Certification of critical components

According to § 165(4) TKG, critical components within the meaning of § 2(23) BSIg may only be used by an operator of public telecommunications networks with an increased risk potential if they have been checked and certified by a recognised certification body before being used for the first time. The certification of the critical components must be based on the TR-03163 of the BSI.

If no possibilities for certification are available at the time of the first deployment of a critical component or if the deployment takes place before the cut-off date rule (see subchapter below), obligated system operators and service providers must take appropriate and appropriate technical precautions and other security measures when deploying critical components.

Product certification specifies requirements for the operating environment or the safe operation of products. Only by complying with these specifications belonging to the certificate can a certificate-compliant operation of the component be guaranteed.

5.2.1 Transitional regime for the certification of critical components

With regard to the requirements for the use of certified critical components, the following transitional arrangement shall apply until the cut-off date specified below:

deadline

The cut-off date for the respective critical component shall be the last day of the 24th month at the latest after the certification of the product to which the respective critical component belongs is possible for the first time in accordance with TR-03163 of the BSI, but no earlier than 01.01.2026. The possibility of certification requires both the publication of TR-03163 and the availability of product-related requirements documents. The TR-03163 is published on the BSI website (www.bsi.bund.de) together with a reference to the relevant requirements documents and the reference date for the product type. For the calculation and compliance with the reference date, it is irrelevant if the documents for certification (TR-03163 or the corresponding requirement documents) are exchanged or updated.

Use of existing components up to the reference date

Until the end of the reference date, the first use of critical components not previously verified and certified by a recognised certification body ('inventory component') without certification shall be permitted.

The certification obligation thus refers to the first use of a single critical component after the reference date. This also applies if the type and type of initial use of a critical component corresponds to that of the existing component.

Existing components already in use do not have to be certified retrospectively.

5.3 diversity

When planning and setting up networks, 'monocultures' should be avoided as far as possible. This can be achieved by using components from different manufacturers. These manufacturers should be independent of each other and not dependent on a third party. In particular, critical components should not be dependent on a single manufacturer of critical components due to the implemented network topology. Networks must be topologically designed in such a way that diversity also applies to sensitive network functions and network elements that require particular protection. As the state of the art evolves, the interoperability of interfaces of network components should be in place, in compliance with technical standards, in order to further enhance diversity.

Measures must be developed to compensate for the short-term unavailability of components from a manufacturer in order to maintain the functionality of the network.

5.4 Technical measures for security in 5G networks

5G envisages improvements in security features compared to previous generations.

The standard provides several options to enable operations to comply with various government regulations. The selection or activation is carried out in accordance with the regulatory requirements, or at the choice of the respective network operator, if no national regulation or other legal framework conditions exist.

For the relevant obliged entities of this general provision, the following measures shall ensure that these features are activated on all 5G public networks.

5.4.1 Protection of the identity and privacy of participants

The identity of the user must be protected from disclosure in order to prevent tracking and identification of the user. The secret authentication information and key cryptographic material shall be adequately protected.

Legitimate purpose

The legitimate purpose is to protect participants' identities, confidentiality, authentication information and cryptographic key material from disclosure.

Appropriateness

The definition and implementation of specific technical measures is an appropriate means to protect the identity of the subscribers, confidentiality and authentication information, in particular protection measures in the form of encryption. Defining and implementing measures to protect the cryptographic key material itself is an appropriate means of ensuring effective encryption.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

The described Subscription Permanent Identifier (SUPI) / Subscription Concealed Identifier (SUCI) encryption measure is a basic security feature of 5G technology, in particular to protect the confidentiality of subscriber identity on the air interface³⁵³⁶. Participant identities form the basis for the provision of the service and their confidentiality is indispensable for the achievement of the security objectives described above.

The described measure for authentication and key derivation was already introduced in the third mobile phone generation (3G) and serves, among other things, to protect against fraud on the mobile phone operators. This measure is therefore also in the self-interest of the operators.

³⁵ <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf>

³⁶ <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Security%20in%205G%20Specifications.pdf>

The described measure to protect the encryption information protects the confidentiality of the communications of all users of an operator by keeping the cryptographic material used for the encryption of the communications secure. If this becomes known, an attacker can decrypt any communication of his victim. Recorded data can also be decrypted subsequently.

In a high-level/hardware security module, the cryptographic material is tamper-resistant, tamper-proof and access-proof.

In order to minimize the impact on performance through cryptographic computing operations, a high-level/hardware security module (HSM) can be used, which is designed for particularly valuable security-relevant information (master keys, keys of global importance, etc.) and for very high performance requirements.

The described measure for the regular renewal of the short-term user ID protects the identity and information on the position of the user on the air interface. This measure, together with SUPI/SUCI encryption, is thus an effective protection against tracking by signalling data on the air interface. The ETSI 5G standard already requires mandatory renewals for most cases where the 5G Global Unique Temporary Identifier (5G-GUTI) should be renewed.

According to the "periodic registration update", unlike other events to which the 5G-GUTI is sent, there is no obligation to renew, but is recommended in the standard according to³⁷. "periodic registration update" is carried out regularly, the period is freely selectable. Failure to carry out the renewal may lead to inferences as to the identity and position of the user.³⁸

According to current knowledge, there are no other measures, other than those described here, to achieve the protection objective.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The cost of the SUPI/SUCI encryption measure is not disproportionate to the objective of protecting the confidentiality of communications. In particular, sufficient equipment is available on the market to meet the requirements. The technical requirement for this requirement has already been implemented by all manufacturers that comply with ETSI TS 133.501 paragraph 5.2.5 + C.3.4.1, as the standard provides for mandatory implementation and optional activation of the measure. Ideally, the obliged entity only needs to activate the measure.

The measure is already partially rolled out. Furthermore, a well-known terminal manufacturer has already prevented the support of dial-ins to the 5G SA network if SUPI encryption does not take place.

³⁷ <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf>

³⁸ <https://fight.mitre.org/techniques/FGT5012.003/>

The GSMA, as the international advocacy body for mobile operators, also recommends that zero encryption should not be used.³⁹ In⁴⁰ the 5G security report, one of ENISA's key recommendations is to avoid zero encryption.

The described measure for authentication and key derivation has already been applied at least partially in 3G.

The GSMA, as the international advocacy body for mobile operators, recommends the support of MILENAGE and TUAK⁴¹.

The burden for obliged entities associated with this measure to protect encryption information is also not disproportionate to the purpose pursued.

In⁴² the 5G security report, one of ENISA's key recommendations is to implement the measures listed here to secure authentication and key derivation and to protect encryption information.

The implementation of this measure to protect the cryptographic material is also in the self-interest of the operators.

The technical prerequisite for the regular renewal of the short-term user ID has already been implemented by all manufacturers who are standard-compliant with ETSI TS 133.501 paragraph 6.12.3. Ideally, the obliged entity only needs to activate the measure.

Since the renewal already takes place in other cases, such as Registration Request message of the type "initial registration", "mobility registration update", as well as Service Request, leaving the 5GMM-IDLE state⁴³, and thus the costs of implementation in this further case are low, the costs of the measure are not disproportionate to the benefits achieved.

Encryption of the permanent user ID

Whenever possible, the permanent user ID Subscription Permanent Identifier (SUPI) should not be transmitted in plain text, but in encrypted form as a Subscription Concealed Identifier (SUCI).

Safeguard measures:

- The operator must ensure the encryption of the SUPI to the SUCI for all connections and connection attempts between terminal devices with a USIM provisioned for its own network and a 5G core network

³⁹ <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf>

⁴⁰ <https://www.enisa.europa.eu/publications/security-in-5g-specifications>

⁴¹ <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf>

⁴² <https://www.enisa.europa.eu/publications/security-in-5g-specifications>

⁴³ ETSI TS 133.501

- Encryption with the NULL scheme does not provide protection for the participants and is therefore not permitted, except in the case of mandatory legal reasons or regulatory requirements
- The use of Profile A based on Curve25519 according to [3GPP TS 33.501] Annex C.3.4.1 is recommended

Secure authentication and key derivation

For authentication and key derivation algorithms, evaluated and appropriate publicly investigated algorithms shall be used.

Safeguard measures:

- The use of the publicly analysed algorithms MILENAGE ([3GPP TS 35.205]) together with the 'default parameters' or TUAK ([3GPP TS 35.231]) mentioned therein is recommended (see also GSMA Official Document FS.35 - Security Algorithm Deployment Guidances Version 4.0)
- For basic requirements for algorithms, the technical guideline BSI TR-02102-1 "Cryptographic methods: Recommendations and key lengths"

Protection of encryption information

As a root of trust for the security functions in the network, the cryptographic material used (keys and algorithms) must be centrally stored or executed in a tamper-proof and burglary-proof manner.

Protective measure:

- The operator must ensure that persistent keys and encryption algorithms are centrally stored and executed in the core network in a tamper-proof and burglary-proof manner and that only cryptographically suitable random number generators are used.
- The use of a High-Level/Hardware Security Module (HSM) is recommended

Regular renewal of the short-term user ID

To protect against spying, the short-term user ID for network access must be renewed at regular intervals.

Safeguard measures:

- The operator shall ensure that the 5G core network function AMF renews the short-term user ID 5G-GUTI and sends it to the subscriber device also in the case of 'periodic registration update' (see [3GPP TS 33.501] 6.12.3).
- The 3GPP standard recommends a period of 54 minutes in [3GPP TS 24.501] (T3512). As far as technically possible, this period should not be exceeded.
- The operator must ensure that the 4G core network function Mobility Management Entity (MME) is configured analogously for the renewal of the GUTI (see [3GPP TS 33.401] GUTI, Tracking Area Update (TAU))

5.4.2 Protection of the confidentiality of utility and signalling data

Usage and signalling data between the user and the network must be protected against unauthorised access.

Safeguard measures:

- The operator must ensure the confidentiality of User and Control Plane data between the subscriber terminal and the network through appropriate encryption (User Plane and Control Plane on the Access Stratum; Control Plane on the Non-Access Stratum)
- The selection of the algorithm 128-NEA2 or 128-EEA2 is recommended ([3GPP TS 33.501] D.2.1.3 or 3GPP TS 33.401] B.1.3.) as long as no algorithms with a larger key length are standardized
- The use of the NEA0 or EEA0 (zero encryption / plain text without encryption) is only permitted if there are compelling technical reasons or regulatory requirements

Legitimate purpose

The legitimate purpose is to ensure the confidentiality of the usage and signaling data.

Appropriateness

The definition and implementation of encryption measures is an appropriate means of ensuring the confidentiality of utility and signalling data.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means. According to current knowledge, there are no other measures, other than those described here, to achieve the protection objective.

The measure described protects the confidentiality of the data and the privacy of the user⁴⁴. Exceptions are possible according to the standard for emergency calls, as this can also be done without prior registration on the network.

The GSMA, as the international advocacy body for mobile operators, recommends banning the use of NEA0 and EEA0 zero encryption. As an exception, in addition to emergency calls from an unregistered device, a regulatory encryption ban from the state side is listed⁴⁵. In the 5G security report, one of ENISA's key recommendations is to implement the action listed here. At least 128-NEA1 or a better algorithm should be used. Similarly, use is recommended in the standard in TS 133 501 paragraph 5.3.2 of ETSI wherever regulation allows. The exception for the unregistered emergency call is described in TS 133 501 paragraph 10.2.2 in the standard.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The cost of the action is not disproportionate to the objective of protecting the confidentiality of communications. In particular, sufficient devices used in public networks of users are available on the market to meet the requirements. The technical requirement for this requirement has already been implemented by all manufacturers that comply with ETSI (TS 133.501 paragraph 5.3.2). Ideally, the obliged entity only needs to activate the measure.

5.4.3 Protection of the integrity of utility and signalling data

The integrity of the user and signalling data in the traffic between the user and the network shall be ensured.

Safeguard measures:

- The operator shall ensure the integrity of the User Plane Data and Control Plane between the subscriber terminal and the network through appropriate integrity assurance.
- The use of the algorithm 128-NIA2 or 128-EIA2 is recommended ([3GPP TS 33.501] D.3.1.3 or 3GPP TS 33.401] B.2.3.), as long as no algorithms with a larger key length are standardized
- Integrity backup must also be enabled at full-rate when full-rate integrity backup support is signaled by the subscriber terminal
- The use of the NIA0 or EIA0 (zero encryption/clear text without encryption) is only permitted if there are compelling technical reasons or regulatory requirements

Legitimate purpose

The legitimate purpose is to ensure the integrity of the utility and signaling data.

⁴⁴ <https://www.enisa.europa.eu/publications/security-in-5g-specifications>

⁴⁵ <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf>

Appropriateness

Defining and implementing integrity measures is an appropriate means of ensuring the confidentiality of utility and signalling data. Also, the use of zero encryption does not offer any protection and is therefore not a sufficient alternative to the measure.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means. According to current knowledge, there are no other measures, other than those described here, to achieve the protection objective.

The described measure protects the integrity of the utility and signaling data and thus prevents compromise and modification of the data. This also prevents various man-in-the-middle attacks.^{46 47}

The GSMA, as the international advocacy body for mobile operators, recommends banning the use of NIA0 and EIA0 zero encryption. As an exception, in addition to emergency calls from an unregistered device, a regulatory encryption ban from the state side is listed⁴⁸. In the 5G security report, one of ENISA's key recommendations is to implement the action listed here. At least 128-NIA1 or a better algorithm should be used. Likewise, use in the standard is⁴⁹ recommended wherever regulation allows.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The cost of the action is not disproportionate to the objective of protecting the confidentiality of communications. In particular, sufficient equipment used in public networks is available on the market to meet the requirements. The technical requirement for this requirement has already been implemented by all manufacturers that comply with ETSI (TS 133.501 paragraph 5.3.3). Ideally, the obliged entity only needs to activate the measure.

Moreover, the measure does not significantly reduce the quality of the service provided. Scientific considerations of the performance of the individual algorithms in terms of throughput and latency showed no significant impact on throughput. There were reasonable effects on latency.⁵⁰ The standard TS 133.501 paragraph 5.3.3 obliges the support of integrity protection.

⁴⁶ <https://www.enisa.europa.eu/publications/security-in-5g-specifications>

⁴⁷ <https://doi.ieeecomputersociety.org/10.1109/SP.2019.00006>

⁴⁸ <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2022/09/FS.35-v3.0.pdf>

⁴⁹ ETSI TS 133.501

⁵⁰ <https://dl.acm.org/doi/pdf/10.1145/3558482.3581777>

5.4.4 Protect access to network functions on the 5G core network

In order to prevent unauthorized access to network functions and the spread of a compromise from one to other network functions (lateral movement), the 5G core network must be protected accordingly.

Protective measure:

- The operator must ensure access to the services offered by the network functions through authorization at least by means of the OAuth2.0 protocol in accordance with [3GPP TS 33.501] 13.4.1.

Legitimate purpose

The legitimate purpose is to protect the functions in the 5G core network from unauthorized access.

Appropriateness

The definition and implementation of measures of secure authentication according to current standards is an appropriate means to protect the functions in the 5G core network from unauthorized access. The measure mitigates the spread of attacks through "lateral movement" within the core network, in which only requests from authorized components are processed. In the absence of authorization, an attacker can gain access to any network functions and thus access information or block access to services.⁵¹

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means. Authorisation must be used to secure against unauthorised access.

The measure included is necessary because its objective cannot be achieved by any other equally effective means. If the core network were not backed by OAuth 2.0, a 'lateral movement' attack would not be prevented and greater risks would occur more easily.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The technical requirement for this requirement has already been implemented by all manufacturers that comply with ETSI (TS 133.501 paragraph 13.4.1). Ideally, the obliged entity only needs to activate the measure.

Protection against lateral spread is also a security requirement in other industries with similar technology (e.g. cloud providers). OAuth 2.0 is an established method

⁵¹ <https://www.enisa.europa.eu/publications/security-in-5g-specifications>

In the 5G security report, one of ENISA's key recommendations is to implement the action listed here.

5.4.5 Protection of SBA communication in the 5G core network

The open and distributed service-based architecture (SBA) of the 5G core network increases the risk that communication between network functions can be attacked by a compromised function, interface or execution environment. The integrity and confidentiality of communications on the core network shall be adequately protected.

Safeguard measures:

- The operator shall ensure the protection of communications on the 5G core network in accordance with [3GPP TS 33.501] 13.1
- The operator shall ensure that 'Mutually authenticated TLS (mTLS)/ HTTPS' is used unless network security is ensured by other means equivalent to the level of protection.⁵²

Legitimate purpose

The legitimate purpose is to protect communications in the 5G core network from unauthorized access.

Appropriateness

Establishing and implementing confidentiality measures is an appropriate means of protecting communications on the 5G core network from unauthorised access.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

The described measure provides protection against attacks on network functions within the core network.

If mTLS is activated, it offers protection without having to pay attention to physical limits, such as the localization of the underlying hardware, and thus more freedom in load distribution. The location of a functionality is no longer relevant. "Lateral movement", i.e. the spread of attacks is made more difficult even after entering a security perimeter. This principle is called "defense in depth".

Physical protection by structural measures as an alternative to safeguarding the individual network functions, as the standard allows, is not sufficient, since this measure is not effective due⁵³ to various agile operating scenarios, such as automatic load distribution to spatially separated data centers. Furthermore, physical protection loses its effect if an attack can

⁵² This requirement shall take precedence over paragraph 3 and Note 2 in [3GPP TS 33.501] 13.1.0

⁵³ ETSI TS 133.501

successfully penetrate a security perimeter. In addition, due to virtualization, mixing of different security perimeters can occur more quickly.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

If the communication in the core network is unencrypted, there is also the possibility to access sensitive information such as session keys or the long-term user ID through compromised functions or interfaces, which is why the costs for the measure are not disproportionate to the intended protection of the confidentiality and integrity of the communication. In addition, scientific considerations show that the additional latency in operation is negligible. For the initial connection setup, the latency is higher. The additional CPU load and memory usage are also negligible.⁵⁴

TLS is a well-known and well-established protection for website access on the Internet via the https protocol⁵⁵ for many years, see⁵⁶ and for statistics. In addition, it is an established procedure for virtualized environments. In the 5G security report, one of ENISA's key recommendations is to implement the action listed here.

The technical requirement for this requirement has already been implemented by all manufacturers that comply with ETSI (TS 133.501 paragraph 13.1). Ideally, the obliged entity only needs to activate the measure.

5.4.6 Protection of communication between access network and core network as well as between access networks

The confidentiality of communications between the access networks and the core network, as well as between access networks, shall be protected against unauthorised access.

Access networks in this context include radio access networks for 4G and 5G and non-3GPP access networks, provided that these are parts of the 5G network.

Safeguard measures:

- The operator shall secure communication between access networks and the core network by means of transport encryption.
- The operator must secure communication between access networks by means of transport encryption
- For transport encryption, the use of a cryptographic solution is mandatory

Note: Cryptographic methods according to the recommendations of the Technical Guideline TR-02102 of the BSI

⁵⁴ <https://mediatum.ub.tum.de/doc/1740121/1740121.pdf>

⁵⁵ <https://w3techs.com/technologies/details/ce-httpsdefault>

⁵⁶ <https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture>

Legitimate purpose

The legitimate purpose is to protect communications between the access network and the core network, as well as between access networks, from unauthorized access.

Appropriateness

Establishing and implementing confidentiality measures is an appropriate means of protecting communications between the access network and the core network, as well as between access networks, from unauthorised access.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

The described measure provides protection against attacks on the integrity and confidentiality of communications and prevents the compromise and alteration of network data. This makes man-in-the-middle attacks more difficult.

According to [3GPP TS 33.501] paragraphs 9.2, 9.3, 9.4, some interfaces (N2, N3, Xn) already require the mandatory protection of integrity, confidentiality and protection against replay attacks. For the F1-U interface, the technical support of these safeguards for standard-compliant products shall be mandatory, in accordance with [3GPP TS 33.501] paragraph 9.8. The mandatory security of the F1-U interface also protects the user's communication against attacks on confidentiality and integrity.

Non-3GPP access networks under the authority of the operator must also be secured accordingly, as the protocols and basic standards used differ, but the risk assessment is similar.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

In the 5G security report, one of ENISA's key recommendations is to implement the action listed here.

The use of IPSec is an established measure used to secure communication between the access network and the core network.

5.4.7 Protection of communication within an access network

If the functions of an access network are distributed, the communication between these functions must be protected, regardless of whether they are standardized or proprietary interfaces.

Access networks in this context include radio access networks for 4G and 5G and non-3GPP access networks, provided that these are parts of the 5G network.

Safeguard measures:

- The operator must ensure that the safety functions supported in the respective standard are activated. These include:
 - Mutual Authentication
 - Integrity protection
 - Replay protection
 - Confidentiality protection

If several options are available, the choice of the option with the highest level of protection is recommended.

- For interfaces without specified security requirements or for proprietary interfaces within the access network, the operator is obliged to implement its own security measures.

Legitimate purpose

The legitimate purpose is to protect communications within an access network.

Appropriateness

The establishment and implementation of protective measures to activate the security functions are an appropriate means of protecting communication within an access network.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

The measure serves to protect the integrity and confidentiality of communication via the interfaces in the RAN, in particular also in the Open RAN. A lack of protection could compromise and modify network data and facilitate man-in-the-middle attacks.

Lack of authentication and authorisation may render measures to protect integrity and confidentiality ineffective.

A variety of risks and assessments regarding the completeness of the security measures prescribed in the consortium specifications of the O-RAN Alliance are presented in the Open RAN Risk Analysis published by the BSI⁵⁷ and in⁵⁸ the Threat Model of the O-RAN Alliance. It is

⁵⁷ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publications/Studies/5G/5GRAN_risk_analysis.html?nn=1019518

⁵⁸ <https://specifications.o-ran.org/download?id=697>

clear from the risk analysis that the measures to be implemented are not sufficient. With regard to the optional measures, the O-RAN Alliance has been able to implement improvements since the publication of the study. However, further obligations to activate security measures have not been included in the specifications.

Even proprietary interfaces for which no standardized security measures are available must be secured accordingly, as the protocols and basic standards used differ, but the risk assessment is similar.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The further development of the O-RAN system according to the principle of "functionality before safety" requires the extension of the measure also to new interfaces and proprietary interfaces for which no security measures have yet been specified by the O-RAN Alliance. A safeguarding of interfaces is necessary in any case, even if no specifications should exist in the specifications. This is necessary to prevent or complicate attacks.

5.4.8 Protect communication between the 5G core network and non-5G network elements

The 5G core network can be connected to a 4G core network and other non-5G network elements, such as the IP Multimedia Subsystem (IMS), via interfaces that use the DIAMETER or GPRS Tunneling Protocol (GTP) protocols.

Communication through interfaces between the 5G core network and non-5G network elements shall be adequately protected.

Safeguard measures:

- The operator shall ensure the security of interfaces with GTP or the DIAMETER protocol in accordance with [3GPP TS 33.501] 9.5
- The operator shall ensure protection by means of a cryptographic solution, unless security is ensured by other means equivalent to the level of protection. The use of Network Domain Security for IP based protocols (NDS/IP) or (Datagram) Transport Layer Security ((D)TLS) is recommended.⁵⁹

Legitimate purpose

The legitimate purpose is to protect communications between the 5G core network and other non-5G network elements.

Appropriateness

⁵⁹ These requirements shall apply as a matter of priority to the first sentence of paragraph 2 of [3GPP TS 33.501] 9.5.

Setting and implementing standards to protect interfaces is an appropriate means to protect the security of communications between the 5G core network and non-5G network elements.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

The measure is designed to protect the integrity and confidentiality of communications. Other safeguards, such as physical protection through structural measures, are not sufficient due to distributed data centers and virtualization.

DIAMETER and GTP are older standards. Security deficiencies and attack possibilities are known for both.

The GSMA, representing the interests of mobile operators, documents ⁶⁰ far-reaching security deficiencies, which can be attributed, among other things, to unencrypted connections.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The technical requirement for the specification has already been implemented by all manufacturers that comply with ETSI (TS 133.501, paragraph 9.5). Ideally, the obliged entity only needs to activate the measure.

5.4.9 Protection of roaming signalling

Mobile networks of different operators are interconnected, e.g. for roaming (national, international). Roaming signalling to other mobile networks shall be adequately protected.

Safeguard measures:

- Establish and periodically review a process to document direct roaming partners⁶¹
- The operator must protect signalling traffic to other mobile network operators (Public Land Mobile Network/PLMN) from access by third parties
- The operator must ensure that the own SEPP components are configured in such a way that only the TLS variant for N32-f is offered for direct N32 connections in the course of the N32-c session setup.
 - Exceptional cases are those where direct N32 connections between roaming partners should not be possible
 - Direct connections should always be preferred to indirect connections

⁶⁰ <https://www.gsma.com/membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf>

⁶¹ A roaming partner is any other mobile service provider that enables subscribers (subscribers) of the operator to access the network by roaming.

- For indirect roaming connections via intermediaries, PRINS should preferably be used to terminate the N32-c connection with the roaming partner and not with the intermediary. Depending on the technical capabilities of operators and intermediaries in establishing the roaming connection, additional options based on TLS can be applied.
- For indirect N32 connections, the N32-c connection⁶² must be⁶³ terminated with the roaming partner and not with the intermediary. In this case, the PRINS (ALS) variant for N32-f must be offered.
- For roaming partners where it is not possible to establish a direct N32-c (according to TS 33.501) connection, the reasons for this shall be documented.

Legitimate purpose

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The technical requirement for the specification has already been implemented by all manufacturers that comply with ETSI (TS 133.501 paragraph 13.2). Ideally, the obliged entity only needs to activate the measure.

Appropriateness

Setting and implementing standards to protect interfaces and applying encryption are an appropriate means to protect the security of communications for roaming signalling.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

Roaming signalling is a major innovation of 5G to reduce the previous attack potential of roaming.⁶⁴ This works, among other things, by tracking attacks by mobile operators. The measures for documentation are basic requirements that primarily serve to create transparency. This is a prerequisite for identifying the potential attack surface created by the need to offer global roaming and SMS delivery by non-mobile providers (e.g. registration codes to unlock online services). The identification of attack surfaces should also be in the self-interest of the mobile operator.

The transmission routes and security measures on these transmission routes determine the extent to which end users of the home network are exposed to risks posed by third parties worldwide. Certain of these risks exist regardless of whether end-users leave their home

⁶² A roaming connection shall be considered indirect if at least one other undertaking, such as an "intermediary", evaluates and/or intervenes in the signalling traffic on behalf of the operator or on behalf of the roaming partner.

⁶³ An intermediary can be, for example, a roaming hub, an IPX provider or a provider of roaming value added services.

⁶⁴ <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g>

network or not. A poorly secured roaming infrastructure can be used to attack users who do not roam abroad.

Without information about these routes and the companies involved in the intermediation, the MNO cannot adequately respond to specific incidents, for example when it becomes known that a particular intermediary is taking insufficient security measures and thus gaining access to roaming signalling to unauthorised third parties. The documentation of the purposes (N32Purpose) also serves to determine the potential attack surface and, if necessary, to formulate appropriate countermeasures.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The measure only interferes to a limited extent with the commercial freedoms of mobile operators. The described documentation requirements only concern information that mobile network operators must already have in order to be able to perform roaming at all.

This measure to secure communication via the N32 interface is significantly advanced in the GSMA and was therefore also referred to as the self-interest of the mobile network operator, as it is necessary to secure interfaces.

5.4.10 Protecting Remote SIM Provisioning

The process of Remote SIM Provisioning (RSP) must be adequately protected. To this end, the GSMA has established a uniform approach based on established industry standards.

Safeguard measures:

- Only GSMA SGP.25 or BSI-CC-PP-0100-2018 CC EAL4 + AVA_VAN.5 certified embedded Universal Integrated Circuit Card (eUICC) products pre-personalised in a GSMA SAS-UP tested environment may be sampled⁶⁵ by the background systems in the field using RSP. These background systems must be tested in return by GSMA SAS⁶⁶-SM

Legitimate purpose

The legitimate purpose is to protect the process of providing profile data to the end user. This profile data is uploaded to the end user's eSIM.

Appropriateness

Setting and implementing standards to protect processes and interfaces is an appropriate means to protect the security of communications during remote deployment.

Necessity

⁶⁵ GSMA SGP.21, SGP.22, SGP.23-1, SGP.23-2, SGP.23-3, SGP.24

⁶⁶ GSMA FS.04, FS.05, FS.08, FS.09, FS.18

The measure is necessary if its objective cannot be achieved by another equally effective means.

The data worthy of protection are the profile data, which are created by the mobile network operator or commissioned third parties. These must be transmitted securely to the end device and are stored in the eSIM. The channel for the transmission must be secured.

There are no other measures, other than those described here, to achieve the protection objective, according to the current state of knowledge.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

The measure described has already been implemented by the mobile network operators. Mandatory regulation therefore does not create any additional costs. A deviation from these sensible requirements should be prevented.

The CC certification of eUICC is currently accepted by the industry as appropriate, as a high level of trust between different providers of eUICCs (manufacturers) and users (MNOs) must be achieved.

The documents referred to in the measure were prepared and supported by the GSMA, which represents the interests of mobile operators, with the participation of mobile operators themselves.

5.4.11 Protection against attacks on the execution environment during virtualization and containerization

Virtualized (VNF) or containerized (CNF) 5G network functions must be protected against threats and attacks related to the execution environment.

Safeguard measures:

- The execution environments of VNF and CNF are to be secured according to the state of the art, whereby the fulfillment of the requirements in case of increased protection requirements according to the IT baseline protection is⁶⁷ recommended

Note: There are comprehensive ETSI recommendations on 5G-specific protection of virtualised and containerised environments⁶⁸.

Legitimate purpose

The legitimate purpose is to protect the virtualized (VNF) or containerized (CNF) 5G network functions in their execution environment.

⁶⁷ BSI IT-Grundschutz-Bausteine, Edition 2023; Components SYS.1.5 "Virtualization" and SYS.1.6 "Containerization"

⁶⁸ ETSI ("work in progress") NFV_SEC023 and NFV_SEC025

Appropriateness

Setting and implementing standards to protect the execution environment of CNF and VNF is an appropriate means to protect communication to and between the corresponding network functions.

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

Due to insufficient protection of the virtualization layer and the container, the achievement of the protection targets during attacks is endangered. For example, in the case of 'Kubernetes', the default settings include wide-ranging vulnerabilities and attack possibilities.⁶⁹

Basic IT protection measures are necessary as their objective cannot be achieved by any other equally effective means. Companies with increased risk potential must implement holistic standards, regularly review and update them to ensure that all virtualized and containerized systems are operated and managed. Only by defining such strategies in advance can it be ensured that networks and services are maintained at all times.

The measures are necessary because virtualization and containerization are central components of modern network functions, in the context of 5G network functions, because the attack surface is significantly increased by missing or inadequate protections and security incidents in such environments can have serious consequences for the entire IT infrastructure.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

In particular, the measure does not restrict the operator in the choice of options for hedging.

There are comprehensive recommendations, including from ETSI, for securing virtualised and containerised environments.^{70 71} In addition, the GSMA, representing the interests of mobile operators, recommends⁷² basic security measures for virtualisation and containers in document FS.31.

⁶⁹ Hacking of Kubernetes in standard protection: 5G hacking just got a lot more interesting (Karsten Nohl)
https://program.mch2022.org/media/mch2022/submissions/8BEFCG/resources/220723.OpenRAN_Security-MCH2022_Karsten_Nohl_yKotUaV.pdf

⁷⁰ ETSI GS NFV-SEC023 - Container Security Specification
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58647

⁷¹ ETSI GS NFV-SEC025 - Secure E2E VNF & NS Management
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59208

⁷² FS.31 GSMA Baseline Security Controls
<https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/06/FS.31-Baseline-Security-Controls-v3.0.pdf>

The measure to apply IT baseline protection⁷³ is appropriate as the intended purpose is not disproportionate to the seriousness of the interference. The required standard for securing the execution environment is based on the importance of the public 5G mobile network for the common good in Germany. Therefore, the minimum requirement according to the standard security of the basic IT protection is appropriate, as the basic security would be too low for a KRITIS sector.

5.4.12 Protection when using virtualization or cloud services

In the case of partial or full use of an execution environment or network functions of third parties, such as the use of public cloud services, the 5G network must be protected against the resulting attack vectors and availability risks.

Safeguard measures:

- The operator must demonstrate through technical and organizational measures that the confidentiality and integrity of subscriber data and communication are guaranteed at all times.
- The operator shall demonstrate that the use of third-party services does not reduce the availability or the level of security of the 5G network.
- If the operator outsources functions and data to third parties that are necessary for network administration and network configuration, the operator must also maintain these functions and data under its own jurisdiction.
- The operator shall demonstrate an exit strategy and implement procedures capable of compensating for the partial or complete failure of a third party's services without undue delay, without violating legal or regulatory availability requirements and, where appropriate, without the involvement of that third party.
- It is recommended not to outsource to third parties that are not exclusively subject to national and European law
- It is recommended not to allow the third party to use infrastructure sites outside the EU and ideally to limit them to Germany. This recommendation also applies to the actual place of work of all administrators

Legitimate purpose

The legitimate purpose is to protect third parties in the event of partial or complete outsourcing of the 5G execution environment, in particular when using data centers or cloud services that are not under the sole control of the network operator.

Appropriateness

Establishing and implementing measures to protect the 5G execution environment, including using third parties to protect the confidentiality and integrity of communications, are appropriate means.

⁷³ BSI IT-Grundschutz-Bausteine, Edition 2023; Components SYS.1.5 "Virtualization" and SYS.1.6 "Containerization"

Necessity

The measure is necessary if its objective cannot be achieved by another equally effective means.

A use of public cloud services is not technically necessary for mobile phone operation, but possibly a business decision (outsourcing). Other technical means to achieve the legitimate purpose are given, for example, by the self-hosting of the corresponding network functions. However, if the network functions are outsourced, the security objectives cannot be achieved by equivalent means.

Securing high availability can also be achieved through self-hosting. If the operator decides to use the service of third parties, a corresponding availability must be contractually stipulated, which must not be less than in the case of self-hosting.

The provision of data and functions under its own jurisdiction despite outsourcing to third parties is necessary to ensure availability in the event of exit under stress. This ensures the availability of the network even if the data cannot be extracted in the cloud and cannot be accessed. This measure is necessary in order to be able to execute an exit strategy in an emergency.

An exit strategy is necessary, as otherwise the operator transfers the power of action over its own network to the cloud operator and thus depends on the cloud operator to the extent that functions have been outsourced. This applies to availability and cost-effectiveness.

adequacy

The measure is appropriate if the intended purpose is not disproportionate to the seriousness of the interference.

Security with regard to confidentiality and integrity is generally necessary, as the confidentiality and integrity of subscriber data can be viewed, changed and reused by the cloud operator in the event of insufficient security.

The transfer of data to the cloud must not deteriorate availability compared to availability in self-hosting, otherwise self-hosting must be chosen.

The creation of an exit strategy, including the provision of data and functions under its own authority, ensures the availability of the network in the event of unavailability of data in the cloud. This measure ensures that availability is not significantly worsened by a cloud outage compared to self-hosting.

6. Recommendations and hints

6.1 Local broadband 26 GHz

The allocation holder shall be responsible for protecting its telecommunications infrastructure against attacks and shall bear the risks for the availability of its telecommunications services. This "Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data" can be used as an aid to achieving protection; It is mandatory for public radio networks.

6.2 Underlying norms, standards and guidelines

The safety objectives and measures described in this document have been derived from existing standards and information standards. These can be used to implement the requirements of the catalog. They include examples of protection measures, 5G threat scenarios and describe hazards and measures in the IT-TK environment.

The figure below gives an overview of the associated norms, standards and guidelines.

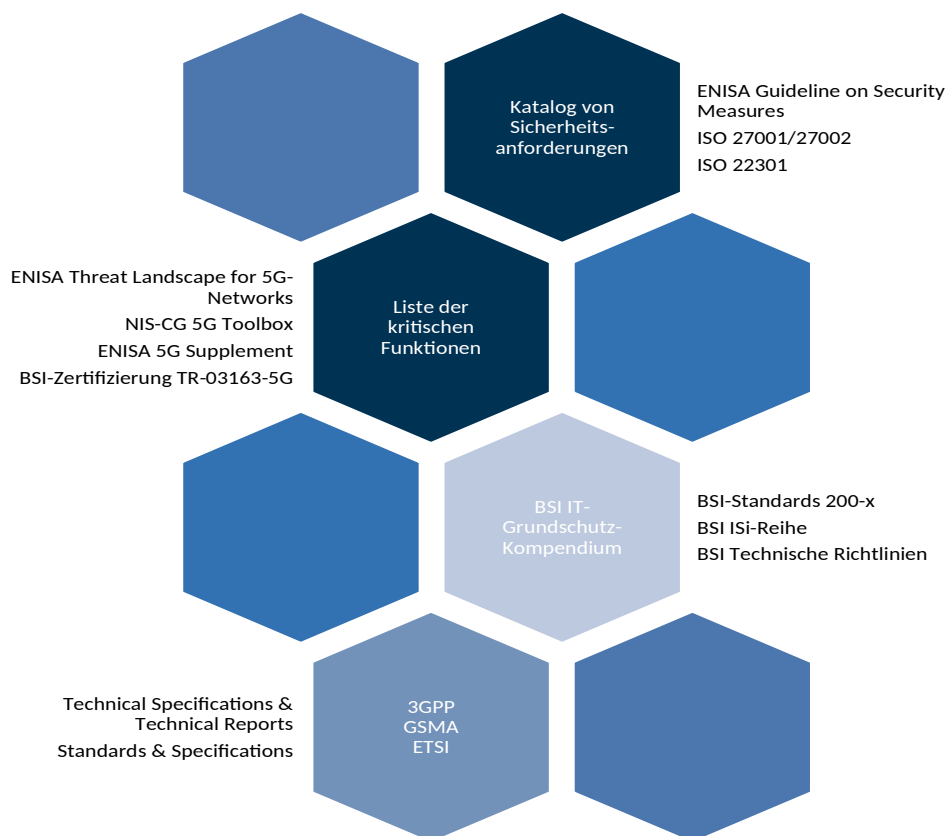


Figure1: Norms, Standards and Guidelines

Glossary

DIAMETER

Authentication, authorization and accounting protocol.

gNodeB

A 'next Generation Node B' is the actual 5G base station that provides user plane and control plane for communication with the 5G subscriber terminal.

GTP (GPRS Tunneling Protocol)

IP-based tunneling protocol.

N32-c

Control Plane interface between SEPPs, to perform the initial handshake and to negotiate the parameters that apply to the actual N32 message forwarding

N32-f

Forwarding interface between the SEPPs used for routing communication between the network service consumer (NF service consumer) and the network service producer (NF service producer) after application-level security protection is applied.

PAM

Privileged access management, security strategy to limit privileged access to what is necessary

Replay protection

Protection against a cyber attack in which network packets are intercepted and repeatedly imported

SLA

Service level agreement, an agreement on the quality and price of a service contract

List of abbreviations

5G NSA	Non-Standalone
5G SA	Standalone
BDSG	Federal Data Protection Act
BEREC	Body of European Regulators for Electronic Communications
BfDI	Federal Commissioner for Data Protection and Freedom of Information
BNetzA	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways
BR-Drs.	Printed matter of the German Federal Council
BSI	Federal Office for Information Security
BSIG	Act on the Federal Office for Information Security (BSI Act)
BSI-KritisV	Ordinance for the determination of critical infrastructures according to the BSI Act (BSI CRITICAL Ordinance)
BT-Drs.	Bundestag printed matter
CER	Critical Entities Resilience
CSA	EU Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communication Technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act)
GDPR	General Data Protection Regulation
(D)TLS	(Datagram) Transport Layer Security
EECC	European Electronic Communications Code
ENISA	European Agency for Cybersecurity (formerly European Network, Information Security Agency)
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit Card
GTP	GPRS Tunneling Protocol

GSMAGlobal System for Mobile Communications Association

GSMA SAS-UPGSMA Security Accreditation Scheme for Universal Integrated Circuit Card (UICC) Production

GSMA SAS-SMGSMA Security Accreditation Scheme for Subscription Management

GUTIGlobal Unique Temporary Identifier

HTTPS Hypertext Transfer Protocol Secure

IT Information technology

SMEMicro, small and medium-sized enterprises

MANOManagement and network orchestration

MECMulti-access edge computing

MMEMobile Management Entity

MNOMobile Network Operator

NDS/IPNetwork Domain Security for IP based protocols

NFNetwork function

NFVNetwork functions virtualization

RANRadio Access Network

RSPRemote SIM Provisioning

SEPPSecurity Edge Protection Proxy

TDDDGTelecommunications Digital Services Data Protection Act

TKtelecommunications

TKGTelecommunications Act

TRTechnical Directive

C Annex 1 - Technical specification for packet switched networks to the Safety Requirements Catalogue

1. introduction

The connection of an operator network to the Internet or the provision of telecommunications services on the Internet entails considerable potential danger for the connected telecommunications, computer systems and their users.

An overview of current risks can be found, for example, in the annual management reports of the BSI⁷⁴ and ENISA.

Due to this specific threat situation and due to the importance of the Internet in the business and private sector, appropriate security precautions must be taken by the operators and providers of packet-switched networks. The Annex describes - in addition to the requirements of the main part of the catalogue of safety requirements pursuant to § 167 TKG (Safety Catalogue) - technical precautions and other measures to be implemented for packet-switched networks (Internet) in accordance with the current state of the art. These measures also serve to protect the secrecy of telecommunications or to prevent personal data breaches.

Additional recommendations can be found, inter alia, in the Internet Security Series (ISi Series) and the Cybersecurity Recommendations for Internet Service Providers of the BSI.

The focus on technical aspects makes it necessary in this annex to the Safety Catalogue to use terms that are essential to describe the state of the art on the one hand, but which are not used in the TKG on the other hand. These terms are further explained in the definitions at the end of the Annex.

As in the Safety Catalogue (Chapter 3), the Annex distinguishes between three categories of hazard potentials.

Obligations in the different hazard potentials:

- **Normal hazard potential** (hereinafter referred to as a): All public telecommunications networks and publicly available telecommunications services
- **Increased risk potential** (hereinafter referred to as b): Public telecommunications networks and publicly available telecommunications services, where they are of greater importance for the common good

⁷⁴ <https://www.bsi.bund.de/lagebericht>

- **Increased risk potential** (hereinafter referred to as c): Public telecommunications networks and publicly available telecommunications services, provided that they are of paramount importance for the common good

2. Distributed Denial of Service (DDoS) attacks

DDoS attacks can cause considerable damage. Obligated entities play a central role in mitigation and help reduce the risk and impact of successful DDoS attacks.

2.1 Improvement of your own infrastructure

Many DDoS attacks resemble peak loads in their symptoms. A simple way to successfully withstand small and medium-sized DDoS attacks is therefore to have sufficient capacity ready.

a)

- No mandatory measures foreseen

b)

- Capacities of own infrastructure and exchange points must be sufficiently sized to individually ensure the availability of the comprehensive network in the event of a small and medium strength DDoS attack

c)

- No additional measures are obligatory for this point

2.2 Mitigation

If a DDoS attack exceeds the spare capacity, the incoming traffic must be specifically discarded or cleaned up.

a)

- No mandatory measures foreseen

b)

- In order to protect the own infrastructure and the connected customers, there must be a possibility to filter/clean up the attack traffic

c)

- No additional measures are obligatory for this point

2.3 Securing exploitable systems

Many Internet services can be misused for DDoS attacks. Typical examples include Domain Name System (DNS) and Network Time Protocol (NTP) servers, where responses are often many times larger than requests. Thus, these Internet services can be exploited as amplifiers in DDoS attacks.

a)

- Unnecessary services must be deactivated
- In addition to Chapter 4.4.3 of the Safety Catalogue: Access to systems that can in principle be used as reflectors for DDoS attacks (e.g. DNS resolvers or NTP servers) must be restricted to the intended users
- Systems that can in principle be used as reflectors for DDoS attacks must be configured in such a way that the gain factor is as low as possible (e.g. no support "monlist" for NTP)

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

3. Inter-domain routing

The exchange of IP routing information is the prerequisite for the cross-operator data flow. This exchange takes place on the Internet via the exterior Border Gateway Protocol (eBGP, hereinafter BGP).

3.1 Protection of the BGP session

Existing BGP sessions are the prerequisite for exchanging routing information. Therefore, the protection of BGP sessions is of central importance.

a)

- BGP sessions should be protected according to common best practice (such as TCP-AO, GTSM) [RFC7454]
- The TCP session underlying a BGP session should also be protected against attacks using common best practices (such as ACLs).

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

3.2 Provision of routing information

In order to filter incorrect routing information (see appendix, chapter 3.3), the own routing information must be documented.

a)

- Authenticated and authorized routing information must be provided in a standardized form (e.g. using ROAs in RPKI)

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

3.3 Preventing the dissemination of incorrect routing information

Dissemination of incorrect routing information can lead to interference and facilitate attacks.

a)

- Incoming and outgoing routing advertisements from and to BGP neighbors must be checked against an authorized source and rejected or filtered in the event of deviations (e.g. by means of ROV)

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

3.4 Prevent traffic with fake source IP addresses

The basis for many incidents and attacks is the use of fake IP addresses. This can be contained or even prevented by setting up appropriate filters.

a)

- Network operators must implement a source address validation system for their infrastructure, end customers and customer networks (more precisely single-homed stub networks) and filter packets with fake source IP addresses. [MANRS] [RFC2827] [RFC8704]

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

3.5 Providing up-to-date contact information

The following requirements are for network operators to contact each other in the event of an incident:

a)

- Obligated entities should maintain up-to-date contact information in a database (such as the associated RIR/NIR or PeeringDB) [MANRS]

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

4. Domain Name System - Resolver

In order to provide interpersonal communication services, the operation of name resolution systems (Domain Name System) is absolutely necessary. Furthermore, the provision of DNS resolvers is a central service of many telecommunications operators and service providers on the Internet. On the Internet, almost every communication process is preceded by a request to the DNS, so a secure configuration of the DNS resolver is essential.

4.1 Technical requirements

The correct function of the DNS resolver requires, among other things, the following technical requirements:

a)

- DNS resolvers must be able to be addressed via the transport protocols TCP and UDP
- DNS resolvers must support EDNS(0) [RFC 6891]
- DNS resolvers should limit the size of DNS response packets over UDP to 1232 bytes⁷⁵

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

4.2 DNSSEC

The Domain Name System Security Extensions (DNSSEC) security extension allows domain owners to cryptographically sign DNS records and DNS resolvers to validate those signatures. This ensures the integrity and authenticity of DNS records.

a)

- DNS resolvers must validate DNSSEC if the requested domain has a DNSSEC configuration
- In addition to RSA, DNS resolvers must also support current cryptographic methods (such as ECDSA and EdDSA) [RFC 9364]

b)

- No additional measures are obligatory for this point

⁷⁵ <https://www.bsi.bund.de/dok/frag-dns>

c)

- No additional measures are obligatory for this point

4.3 Cache poisoning

Typically, DNS resolvers store the results of requests between (caching) in order to be able to answer new requests more quickly directly from the cache. Attacks to manipulate existing entries or to introduce incorrect entries in this cache are called cache poisoning. To aggravate such attacks, a number of measures have been established that need to be supported by the DNS resolver.

a)

- DNS resolvers must support the randomization of the source port
- It should be possible to set a time-to-live (TL) limit on the DNS resolver
- DNS resolvers should support domain-related early removal of cache records (flushing)

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

4.4 Privacy

DNS requests can contain sensitive information. Various methods have been established to protect this information:

a)

- DNS resolvers must support QNAME Minimization [RFC 9156]

b)

- DNS resolvers should support an encrypted transport option (such as DNS-over-QUIC [RFC 9250], DNS over TLS [RFC 7858], or DNS over HTTPS [RFC 8484])

c)

- No additional measures are obligatory for this point

5. Domain Name System - Authoritative DNS Servers

The nameserver responsible for a particular domain is called the authoritative DNS server. It provides information about the domain name in the form of a DNS zone.

5.1 Technical requirements

The correct functioning of the authoritative DNS server requires, among other things, the following technical requirements:

a)

- Authoritative DNS servers must be accessible via TCP and UDP transport protocols
- Authoritative DNS servers must support EDNS(0) [RFC 6891]
- Authoritative DNS servers should limit the size of DNS response packets over UDP to 1232 bytes⁷⁶

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

5.2 Protection against exploitation

Authoritative DNS servers can be misused as a tool for DDoS attacks. The following measures can be used to regulate the use of the DNS server.

a)

- At the authoritative DNS server, measures must be taken against exploitation for amplification/reflection attacks, such as response rate limiting and the avoidance of fragmented response packets

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

⁷⁶ <https://www.bsi.bund.de/dok/frag-dns>

5.3 DNSSEC

Signing a DNS zone allows the recipient to verify the integrity and authenticity of the information provided. This allows attacks to be detected and, if necessary, prevented. Furthermore, DNSSEC is a mandatory prerequisite for further security mechanisms (e.g. DNS-based Authentication of Named Entities (DANE)).

a)

- No mandatory measures foreseen

b)

- The zones of the authoritative DNS server should be signed with DNSSEC. This is especially true for zones with Mail Exchange Resource Records (MX records) pointing to email servers, as well as the zones of the email servers themselves.
- Authoritative DNS servers should implement current cryptographic techniques, such as Elliptic Curve Digital Signature Algorithm (ECDSA) [RFC 9364]
- Operators of authoritative DNS servers should follow the development of DNS and DNSSEC-related Internet standards

c)

- No additional measures are obligatory for this point

6. Email security

Any transmission of e-mails between e-mail providers and to their users is subject to telecommunication secrecy and must be adequately secured. As a basic measure to protect the secrecy of telecommunications and to protect against attempts at manipulation, e-mail transport must be encrypted. Complementary measures offer protection against malware, phishing and spam - both for their own users and those of other providers.

a)

- For both incoming and outgoing connections to e-mail transport, transport encryption must be offered and, if technically possible, used. The state of the art must be taken into account
- The requirements of BSI TR-03108 Secure e-mail transport are to be implemented
- The requirements of BSI TR-03182 e-mail authentication are to be implemented

b)

- No additional measures are obligatory for this point

c)

- No additional measures are obligatory for this point

Recommendations and notes:

Further measures to protect against malware and to prevent spam and phishing can be implemented taking into account the requirements of the TDDDG and are recommended.

7. Awareness of Threats

Chapter 4.10 of the Security Catalogue sets out security objectives related to threat intelligence and contact with end-users. Corresponding information on the main threats to the security of networks and services shall be shared by obliged entities with their customers. These security objectives, initially outlined in the abstract in the security catalogue, are further specified by the measures listed below for Internet telecommunications network operators and telecommunications service providers on the Internet.

In order to keep the security of networks and services up-to-date at all times, systematic knowledge management should be established. The aim here is to collect as comprehensive information as possible on new threats and defensive mechanics from sources such as manufacturer or computer emergency response team (CERT) messages and to exchange information with other telecommunications providers via the security-related "State of the ART".

Furthermore, information on hazards affecting customers in particular should be passed on to them, together with information on how effective protection against these hazards is possible.

7.1 Establishing Vulnerability Management

Vulnerability management must be established for secure IT operation in order to identify gaps in software, components, protocols and external interfaces of the environment as well as to derive, evaluate and implement the resulting necessary actions.

7.1.1 Systematic collection and evaluation of vulnerability reports from manufacturers and CERTs

a)

- Warnings and vulnerability reports from manufacturers regarding the products used in their own network must be observed, evaluated and the resulting security measures implemented.

b)

- In addition to the notifications from manufacturers, notifications and warnings from relevant CERTs and other sources (public reporting, safety instructions from third parties, MISP, honeypot analyses, etc.) must also be evaluated accordingly and the resulting security measures for their own systems implemented as necessary.
- Furthermore, organisational and technical audits of the own systems for vulnerability analysis must also be carried out on a regular basis.

c)

- No additional measures are obligatory for this point

7.1.2 Exchange of information and cooperation with other providers and operators

a)

- No mandatory measures foreseen

Note: Providers and operators of category (a) shall be open to join the cooperations specified in (b).

b)

- Findings on current attack methods and types (e.g. regarding DDOS, DNS reflection, etc.) as well as appropriate defensive techniques (e.g. filter rules) should be regularly exchanged among each other across providers
- In order to ensure a fast ability to act across providers if necessary, contact persons, accessibility and emergency numbers should be exchanged with each other
- Cross-vendor cooperation should be optimised through regular exercises
- In the event of a crisis, a joint situational centre should be operated.

c)

- No additional measures are obligatory for this point

Definitions of Annex (Technical Specification)

Services within the meaning of the TKG

Under Paragraph 3(1) of the TKG, ‘provider of telecommunications services’ means any person who provides telecommunications services.

Accordingly, the TKG defines the term ‘service’ in the sense of a service provided by a provider.

Technical services

In contrast to the TKG, an ‘internet service’ in the technical sense does not mean a service provided by a ‘provider’, but an application which the internet makes available to the user via its infrastructure. Examples of such services or applications include:

- The World Wide Web (WWW)
- E-Mail
- (VoIP) telephony
- Chat
- ...

Further specialisation is given to the term ‘service’ in the technical field in relation to a specific operating system or server level.

Thus, an operating system such as Unix, Linux, Windows, etc. provides services such as:

- User management
- File system management
- Configuration of the hardware
- Printer sharing

available in the form of ‘utilities’.

Services such as:

- HTTP, HTTPS
- FTP, SFTP
- SMTP, IMAP, POP
- SQL
- ...

on the other hand, servers make them available to ‘clients’ (i.e. client applications or client programs) or their users for the performance of their tasks.

Transit provider

End customers access content and applications provided by content and application providers (CAPs). In order for such content and applications to reach the end-user, the networks involved must interconnect. This is done online via transit or peering. Through transit agreements, a network operator (transit provider) offers other network operators connectivity to the entire Internet for a fee. In peering, network operators exchange traffic only with each other, mostly without payment of charges.

<https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/Schutz/PeeringTransitmaerkte/start.html>

List of abbreviations

ACL	Access Control List
BGP	Border Gateway Protocol
- eBGP	- exterior Border Gateway Protocol
CERT	Computer Emergency Response Team
DANE	DNS-based Authentication of Named Entities
DDoS	Distributed Denial of Service
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
- DNSSEC	- Domain Name System Security Extensions
- EDNS(0)	- Extension Mechanisms for DNS (according to RFC 6891)
- DNS-over-QUIC	- DNS over Quick UDP Internet Connections
DSA	Digital Signature Algorithm
- ECDSA	- Elliptic Curve Digital Signature Algorithm
- EdDSA	- Edwards-curve Digital Signature Algorithm
DV	computing
GTSM	Generalized TTL Security Mechanism
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
MANRS	Mutually Agreed Norms for Routing Security
MTA	Mail Transfer Agent
MX record	Mail Exchange Resource Record
NTP	Network Time Protocol

PeeringDB	Peering Data Base
QNAME Minimization	DNS Query Name Minimisation to Improve Privacy (according to RFC 9156)
RIR/NIR	Regional Internet registry / National Internet registry
ROAs in RPKI	Route Origin Authorizations in Resource Public Key Infrastructure
RSA	Rivest-Shamir-Adleman (asymmetric cryptographic method)
Transmitter ID	Transmitter identification
SPF	Sender Policy Framework
TCP	Transmission Control Protocol
- TCP-AO	- TCP Authentication Option
TK	telecommunications
TLS	Transport Layer Security
- STARTTLS	- Method for initiating a TLS connection
- TTL	- Time to Live
UDP	User Datagram Protocol

D Annex 2 - List of critical functions

1. List of critical functions

The following table (Figure2: List of defined critical functions, § 167(1)(2) TKG) was prepared jointly by BNetzA, BSI and BfDI. For the preparation, the state of the art was taken into account as much as possible. The list shall be continuously updated together, in particular where essential conditions have changed.

The following list refers to 5G network components as well as the systems necessary for 5G network operation. Accordingly, 4G network components and also the systems exclusively necessary for the operation of 4G networks are expressly excluded from the list.

The following functions shall be considered critical because their degradation or failure adversely affects the general availability, confidentiality, authenticity or integrity of the network. This applies in particular if there are relevant attack vectors that can cause a supraregional impairment, e.g. through foreign influence.

Kategorie		Funktion
A	Core network functions (Kernnetzfunktionen) ¹⁾	• Authentifizierungs-, Roaming- und Sitzungsverwaltungsfunktionen für Endnutzer • Datentransportfunktionen für Endnutzereinrichtungen • Zugriffsrichtlinienverwaltung • Registrierung und Autorisierung von Netzwerkdiensten • Speicherung von Endnutzer- und Netzwerkdaten • Verbindung mit Mobilfunknetzen von Drittanbietern • Exposition der Kernnetzfunktionen gegenüber externen Anwendungen • Zuordnung von Endgeräten zu Netzwerk-Slices
B	Network functions virtualization (NFV), Management and network orchestration (MANO)	• Management und Orchestrierung virtualisierter Netzwerkfunktionen
C	Management systems and supporting services	• Sicherheitsfunktionen des Management-Systems • Zertifikatsverwaltung
D	Radio Access Network (RAN)	• 5G-RAN-Management • Funktionen der gNodeB
E	Transport and transmission functions	• 5G-spezifische Sprach- und Datentransportfunktionen in der Backbone Infrastruktur / Rechenzentren
F	Internetwork exchanges	• IP-Netzwerk außerhalb der MNO-Räumlichkeiten (Netzwerkdienste von Dritten) • Firewall Infrastruktur beim Übergang zu Fremdnetzen
1) unabhängig vom Ort der Realisierung innerhalb des 5G-Netzes (z.B. eine Realisierung im RAN oder MEC)		
Quelle: Bundesnetzagentur		

Figure2: List of defined critical functions, § 167(1)(2) TKG

As an interpretative aid to the list of critical functions, please refer to the following additions:

Category A - Core network functions

Basically, all core functions described in the 3GPP architecture model are critical. Furthermore, non-3GPP-specified functions can also represent critical core network functions. Therefore, additions must be made to the practical derivation for the respective network.

By way of example, the following functions are assigned to the core for the individual coats of the list of critical functions in category A:

- End-user authentication, roaming and session management features
 - Access and Mobility Management Function (AMF),
 - Session Management Function (SMF),
 - Authentication Server Function (AUSF),
 - Unified Data Management (UDM)
 - Security Edge Protection Proxy (SEPP)
- Data transport functions for end-user facilities
 - User Plane Function (UPF),
 - Access and Mobility Management Function (AMF)
- Access policy management
 - Policy Control Function (PCF),
 - Unified Data Management (UDM)
- Registration and authorisation of network services
 - Network Repository Function (NRF)
- Storage of end-user and network data
 - Unified Data Repository (UDR),
 - Unstructured Data Storage Function (UDSF),
 - Service Communication Proxy (SCP),

- Network Data Analytics Function (NWDAF)
- Connecting to third-party mobile networks
 - Security Edge Protection Proxy (SEPP)
- Exposure of core network functions to external applications
 - Network Exposure Function (NEF),
 - Application Function (AF)
- Assignment of terminal devices to network slices
 - Network Slice Selection Function (NSSF),
 - Network Slice Admission Control Function (NSACF),
 - Network Slice-specific and SNPN Authentication and Authorization Function (NSSAAF)
- Secure connection to access networks of other standards
 - Non-3GPP Interworking Function (N3IWF),
 - Trusted Non-3GPP Gateway Function (TNGF)

Category B - Network functions virtualization (NFV), Management and network orchestration (MANO)

MANO functions enable the all-encompassing management and orchestration of VNF and CNF in the NFV architecture. MANO instantiates network services by automating, deploying and coordinating workflows to Virtualized Infrastructure Managers (VIM) and VNF Managers. Furthermore, the MANO functions connect the NFV architecture with the existing Operating Support Systems (OSS) / Business Support Systems (BSS).

This also includes the management functions for the infrastructure of virtualized or containerized management functions.

Category C - Management systems and supporting service

Strong attack scenarios exist on all management systems (management systems for the security of the overall system and all subsystems). This is why securing these systems is an important safety factor (access, roles, securing the system itself, etc.).

This category includes all management functions that are not already named in category B or category D. Examples can be given: Element manager of the core network and the transport network.

Category D - Radio Access Network (RAN)

5G-RAN management refers to all management systems for the managed components with RAN functionality, regardless of where in the overall system the respective management system is located. Accordingly, 5G-RAN management includes all system functionalities that can control and control RAN components via interfaces. This also includes all functionalities to make components of the RAN (via AI or ML) intelligent and adaptive.

For example, 5G RAN management includes:

- All network management systems for controlling the RAN (e.g. Performance management and safety management)
- Site Management RAN (integrity, perimeter, availability, etc.)
- Control and parameterization of gNodeB
- Access control and interfaces from core to RAN
- Prioritization of crypto algorithms in the RAN
- RAN Configuration Data Management and Interfaces

In addition, all functions of the gNodeB are to be classified as a critical function, as material impairments of the same have an impact on availability, confidentiality, integrity and authenticity.

Additional features in RAN architectures built on the 3GPP standard or used alternatively, such as Open RAN, may also include critical features.

Category E - Transport and transmission functions

5G-specific voice and data transport functions in the backbone infrastructure of the mobile network operator and data centers of the mobile network operator include functions of transport and transmission of data (implemented, for example, in routers, switches).

Data centers of the mobile network operator are considered to be all data centers where the critical functions are performed. This does not include voice and data transport functions of the access network.

Category F - Internetwork exchange

Peripheral protection plays a central role in securing transitions between the network infrastructure of the MNO and external networks. These interfaces represent a potential weak point, as different network infrastructures with potentially divergent security standards collide here.

It is therefore about all transitions to other network infrastructures outside the actual sovereignty of the MNO. The subject of consideration is the respective interface to the external network, in particular the firewall infrastructure during the transition to the external network. The external network is not the subject of consideration. This is where the security concepts there apply. If vicarious agents are used in this context, the observance of all relevant protective measures must be ensured through legal and contractual provisions.

Exemplary for peripheral protection can be named:

- Use of IP network providers
- IPX Provider
- Roaming Hubs
- Edge Computing
- Internet Exchange Points
- Direct peering with other providers
- Hosted SEPP

In addition to the firewall systems, IDS/IPS must also be named here, which can detect unusual behavior or signature-based threats and actively prevent them.

2. Process for the identification of critical components in the operated network

Operators of 5G public mobile networks shall implement and implement a process for the identification of critical components, based on the requirements set out in this Chapter.

The list of critical functions shall be used to identify critical components. The process described here pursues the goal of achieving a consistent application by all network operators.

The process is integrated into the overall process of creating a safety concept in accordance with § 166(1)(3) TKG.

The process of identifying and certifying critical components, as described here, is independent of the obligation to implement the safeguards set out in Chapter Definition of basic details of the technical precautions and other measures to be taken, taking into account the various hazard potentials, § 167(1)(1) TKG. Operators of public telecommunications networks with increased risk potential cannot circumvent their obligation to identify critical components by using mitigating measures, as these measures only reduce the risk of a security incident, but do not affect the criticality inherent in the component.

The steps for identifying critical components are described below:

Step 1: Identification of network components

After describing the network and determining the hazard potential in accordance with Chapter , all components present in the network Determination of hazard potentials shall be identified for the networks with an increased hazard potential.

The identification of the components of the network shall be carried out by the network operator. This step allows the network operator to adapt to its individual network architecture. In principle, all components present in the network must be considered, regardless of whether critical functions are implemented or not.

Step 2: Identification of critical components using critical functions

Once all relevant components of the network have been defined, the descriptions in Chapter 1 of Annex 2 can be used to identify the components that perform critical functions. Where a component implements a critical function partially or fully, that component shall be assessed as a critical component.

3. Proportionality considerations on the list of critical functions

Legitimate Purpose and Appropriateness

These rules serve the legitimate purpose of ensuring the security of 5G networks and services at all times and of mitigating and mitigating security risks. The rules provided for are objectively capable of furthering that objective.

Necessity

The core 5G network is particularly critical for confidentiality and integrity due to its centralised control functions and the storage of sensitive user data. This also applies to functions of management and orchestration of virtualized network functions (MANO, NFV), as they can intervene deeply in all network areas and configure and monitor the systems.

The Radio Access Network (RAN) is crucial for regional availability. In the 5G network, it is also aggravating that functions are no longer monolithic, but more widely distributed and bundled and controlled in less central places. Attacks and manipulative interventions therefore not only have a regional impact on availability.

Transport and transmission functions also take over elementary safety tasks. Here, the special feature lies in the virtualization and containerization of 5G networks, which are also exposed to special attack vectors.

It is therefore necessary to classify the above functions as critical for the secure and reliable operation of a 5G network.

By classifying it as a critical function, two main measures follow.

The first measure is mandatory certification. Certification is a proven method for obtaining an independent evaluation of a component necessary for maintaining function. The second measure may be a procedure under § 41 BSI (prohibition of the use of critical components).

Classification as critical functions due to the possible impairment of public policy or public security is therefore without alternative and thus the most lenient means.

adequacy

Mobile communications are an important pillar for the maintenance of state sovereignty, the protection of citizens' privacy and availability for business and emergency services. In particular, the advanced possibilities of a 5G network will be essential for the above-mentioned tasks in the coming years and therefore need special protection.

To this end, critical functions for availability, confidentiality and integrity have been identified, which must be based on a specific level of protection. These were divided into different categories in order to take into account the different hazards in the respective network areas.

Functions are classified as critical because their manipulation or failure can compromise far-reaching parts of the network.

For this purpose, the BSI has⁷⁷ commissioned various risk analyses, which determine the criticality of the above functions and highlight the necessary protective measures. In addition, the Commission Communication on the implementation of the 5G Cybersecurity Toolbox,⁷⁸ in conjunction with the Europe-wide coordinated risk analysis of 5G network security, highlighted⁷⁹ the importance of implementing safeguards to secure critical elements of communication networks. General European developments show that many Member States - including France, Finland, Sweden, Lithuania, Portugal, Spain and Croatia - have identified and defined critical functions in telecommunications networks. Given the high level of protection and the limited intensity of intervention, the scheme is not disproportionate and therefore proportionate.

⁷⁷ https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/5G_Risikoanalyse/5G_Risikoanalyse_node.html

⁷⁸ <https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox>

⁷⁹ <https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>

Vconsultation

Manufacturers, associations of telecommunications network operators and associations of providers of publicly available telecommunications services had the opportunity to comment on the draft catalogue of security requirements (version 2025-10) initially by 19.12.2025.

Due to the scope of the draft as well as the coincidence in time with the entry into force of the Act on the Implementation of the NIS 2 Directive and on the Regulation of Essential Principles of Information Security Management in the Federal Administration on 6 December 2025, the Federal Network Agency had extended the deadline for consultation until 16 January 2026.

In the course of this consultation procedure on the safety catalogue pursuant to §167 TKG, the Federal Network Agency received 24 comments from companies, manufacturers, associations and institutes.

Of these, four were comments from producers, four from institutions, nine from companies and seven from associations.

In the course of reviewing the comments, the Federal Network Agency identified and identified the following key points of the feedback:

Inclusion of functions of gNodeB in the list of critical functions

In its assessment, the Federal Network Agency was guided by the evolving network architectures and new functionalities of the gNodeB as well as the 5G toolbox and BSI-5G risk analyses.⁸⁰⁸¹

While one of the four manufacturers is clearly against expanding the list of critical functions, the other three are clear supporters. As expected, the main criticisms of the negative position would be disproportionate costs and regulatory burdens, which would have a negative impact on the development of the digital ecosystem in the long term. The other manufacturers emphasize the integral part of the end-to-end security architecture and point to the relevance of the RAN for the entire network.

⁸⁰ https://www.bsi.bund.de/EN/Service-Navi/Publications/Studies/Safety_requirements_5G_mobile_networks/Safety_requirements_5-Mobile_networks.html

⁸¹ https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/5G_Risikoanalyse/5G_Risikoanalyse_node.html
Version 2026-09

All operators reject the inclusion of the functions of gNodeB in the list of critical functions as disproportionate. The management-like functions of gNodeB in the context of the subdivision into Central and Distributed Unit are currently not state of the art. The operators argue that the functions of gNodeB remained unchanged in the standardisation and therefore lack a justification for inclusion in the list of critical functions. Furthermore, the effect of a failure of a single gNodeB would be locally limited. The additional costs of the certification obligation associated with the inclusion of gNodeB in the list of critical functions were also mentioned.

The associations generally warn against taking the list too far. They call for a focus on components that are proven to be responsible for the control, authentication and secure operation of the 5G mobile network. The deletion of the possibility of a case-by-case decision by which a potentially critical component could be classified as uncritical is also rejected. In addition, attention is drawn to a possible impact on the public service contracts of the BMI with the 5G network operators and to the efforts made by the certification obligation, which arises from the inclusion of the functions of gNodeB in the list of critical functions.

On the basis of the comments, the Federal Network Agency has clarified the passage in the list of critical functions on the RAN, but maintains its basic assessment. In the new form of radio networks, the base stations in the RAN assume central functions as security and control elements and are to be classified as critical with regard to the protection objectives of confidentiality, integrity and availability. This applies in particular if there are relevant attack vectors that can cause a supraregional impairment, e.g. through foreign influence.

Classification of hazard potentials

Due to the lack of a legal basis, one company expressly opposes a three-tier system based on the size of the company; another company criticises the classification of criticality on the basis of the mobile phone generation, which is contrary to the principles of technological neutrality and proportionality. Another company is of the opinion that the classification based on company size partially loses a risk-based approach. Two other opinions are that companies with very different criticality and systemic relevance are placed in the same, highest risk category. This contradicts the risk-based approach of regulation.

One association is concerned about the proportionality of the current draft safety catalogue. The risk potentials used were not sufficiently specified and set out in too general a manner. Another association states that the BSI once again differentiates the subgroup of 'operators of critical installations' within the 'particularly important entities'. In contrast, there is no differentiation in the draft between critical plants, which are defined in the KRITIS Roof Act, and particularly important institutions. Another association argues that, regardless of the size of the company, only operators of critical installations who would also be covered by the KRITIS Regulation should be classified in the category of increased risk potential.

When relying on company sizes, the Federal Network Agency follows the approach of the NIS2 Directive, whereby a separate category of protective measures has also been created for micro-enterprises. Thus, the design of the safety measures to be implemented by the obliged entities in the safety catalogue is based on the classification of the respective company in now one of three hazard potentials.

The parameters on the basis of which the classification takes place are turnover and company size. In addition, 5G network operators occupy a special position by already being classified in the highest risk potential level, regardless of company size and turnover. In doing so, the Federal Network Agency takes into account the importance of the respective telecommunications networks and services and takes into account the special business landscape in the German telecommunications sector, in particular small and micro enterprises.

Annex C 'Technical specification for packet-switched networks in the Safety Requirements Catalogue'

The companies complain about the too high level of detail of the measures. This would maintain obsolete protective measures in areas where technical progress is progressing very quickly. One prefers a specification of protection objectives, which must be achieved by companies taking into account the state of the art.

A company is committed to formulating the requirements in a technology-neutral manner and demands responsibility for results instead of detailed specifications.

An association doubts the adequacy of the mechanisms used for email security. The guidelines should only be formulated as recommendations. Another also assesses the requirements for IP networks as far too specific and detailed. There is a risk that the requirements will become obsolete very quickly.

Another association is concerned about the provisions of the Catalogue on IP networks annexed to the Catalogue; from their point of view, there should be no conflicting requirement with regard to the protocols and/or security standards to be used from EU and national regulation.

One institution also criticises the fact that, in the present draft text, there may be an unnecessary restriction on the procedures to be applied. In particular, the chapter on e-mail security will be discussed.

In principle, the Federal Network Agency supports the more liberal approach put forward by the industry not to become too detailed in the specifications. A sensible graduation of the level of detail has the advantage that the regulations do not become obsolete too quickly.

In this respect, the Federal Network Agency has reduced the level of detail of the measures and partially mitigated their obligatory nature. In particular, the measures in the Annex on e-mail security have been designed as a mere recommendation and have no binding effect. Reference is made to the 'state of the art'. "State of the art" is not a rigid term, but corresponds to the current state of technical development and is therefore to be understood dynamically.

directories

List of illustrations

Abbildung 1: Normen, Standards und Guidelines.....	103
Abbildung 2: Liste der festgelegten kritischen Funktionen, § 167 Abs. 1 Nr. 2 TKG.....	127

Disclaimer

publishers

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways
Tulip field 4
53113 Bonn

contacts

Unit 217
At the Meet 40
66123 Saarbrücken
217.Postfach@bnetza.de
www.bundesnetzagentur.de
Tel. +49 228 14-0
Fax +49 681 9330-734

Stand

September 2026

pressure

[Federal Network Agency or printing company]

Photo credits

[List of photographs in alphabetical order]

Text

Unit 217