Bundesnetzagentur

Legal basis and general overview of security requirements in public telecommunications networks

Elena Meiser | Federal Network Agency

08 September 2021

2. 5G Industry Summit

Agenda

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

© Federal Network Agency | Elena Meiser | Elena.Meiser@BNetzA.de

Section 109 (4) of the Telecommunications Act (TKG):

Operators of public telecommunications networks ("TC operators") and providers of publicly available telecommunications services ("TC providers") must draw up a security concept which shows that the security concept is in place:

- which public telecommunications network is operated or which publicly available telecommunications services are provided,
- which hazards are to be assumed and
- what technical protection measures or other protective measures are taken.

Section 109 (4) of the Telecommunications Act (TKG) (continued)

Addressed are technical protection measures or other protective measures

- on the protection of the secrecy of telecommunications, and
- against the violation of the protection of personal data
- to secure telecommunications and data processing systems against unauthorised access and to minimise the impact of security breaches on users or on interconnected networks
- to ensure the proper functioning of networks and thereby ensure the continued availability of the services provided over those networks

Section 109 (6) of the Telecommunications Act (TKG)

- The basis of the safety concept is the **catalogue of security requirements**
- Agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information
- Regular revision and adaptation to changed circumstances (e.g. state of the art)
- European Union elaborations are included in the drafting process

Laws and legal development

IT-SIG 2.0 (as of 5/28/2021):

- Extension/precision of the regulatory regime in § 109 TKG
  - Legal obligation to certify (§ 109 (2) TKG)
  - Creation of a definition competence (§ 109 (6) TKG)
  - Periodic security review by an independently qualified body (Art. 109 Par. 7 TKG)
- Central conceptual starting point "Critical Components“
- Creation of reporting obligations (§ 9b BSIG)
- Manufacturers guarantee declaration (§ 9b BSIG)

IT-SIG 2.0 (continued)

- Extension of the catalogue through the definition of

  - the technical precautions and other measures to be taken, taking into account the various potential hazards

  - Determination of critical functions, which are realized by critical components in the sense of § 2 paragraph 13 of the BSI Act

  - operator of public telecommunications networks with increased risk potential is to be classified

TKMoG (01.12.2021):

- Further obligations and subjects of definition in § 109 TKG

Impact of legal developments

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

Impact of legal developments

- IT-SiG 2.0:

  Disposition of the catalogue of security requirements 2.0 on a new legal basis (§ 109 (6) TKG)

- TKModG:

  Revision of the catalogue of security requirements

  - with regard to new duties and subjects to be defined
  - state of the art

Summary

- Legal anchor in the TKG
- Amendment of the TKG (national implementation of the EECC)
- Creation of a security concept
- The basis of the security concept is the catalogue of security requirements
- Regular review of the implementation of the protective measures by BNetzA

Catalogue of safety requirements

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

Security requirement catalogue

Structure

- Introduction
- Minimum security requirements
- Implementation of security requirements
  - Criticality classification

    Standard criticality: All public telecommunications networks and telecommunications services.

    High criticality: public telecommunications networks and services, provided they are of major importance for the public good.

    Increased criticality: Public telecommunications networks and services, provided they are of outstanding importance for the public good.
- Published as of 12/23/2020 (www.bundesnetzagentur.de/sicherheitsanforderungen)

Security requirement catalogue

- Annex 1
  - Requirements for telecommunications service providers with IP infrastructure
- Enclosure 2
  - Additional security requirements for public telecommunications networks and services with increased risk potential
    - Certification of critical components
    - Trustworthiness of manufacturers and suppliers
    - Security monitoring
    - Instructed specialist personnel
    - Redundancies
    - Diversity

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

incident reporting

- Security breach notification
  - Reporting thresholds:

  - 1 million usage hours affected
  - Interconnection points with international character
  - Emergency call steering
  - Exceptional IT malfunction

  Goal: Continuous adaptation to potential hazards and minimisation of security incidents

- Laws and legal development
- Impact of legal developments on security requirements in public telecommunications networks and telecommunications services
- Catalogue of security requirements
- Incident reporting
- Security in campus networks

Security in Campus Networks

- Campus networks in the 3700-3800 MHz frequency range are for internal communications only; telecommunications services for the general public are not permitted.
- The license holder is responsible for protecting its telecommunications infrastructure against attacks and bears the risks for the availability of its telecommunications services itself
- Users are aware of security aspects in campus networks
- Orientation towards the catalogue of security requirements is recommended for campus networks
- In the 26-GHz-band (24.25-27.5 GHz) campus networks and local public networks can be implemented

Bundesnetzagentur

Thanks a lot!

Elena Meiser | BNetzA | Elena.Meiser@BNetzA.de