Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten

nach § 109 Telekommunikationsgesetz (TKG)

Version 2.0

Herausgeber:

Bundesnetzagentur

Bundesnetzagentur für Elektrizität, Gas,

Telekommunikation, Post und Eisenbahn

Stand: 29.04.2020

---

*Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Inhaltsverzeichnis

1 Systematik, Adressat, Inhalt und Verhältnismäßigkeit der Schutzmaßnahmen

Die ständig wachsende Abhängigkeit der Wirtschaft und der Gesellschaft von der Telekommunikation, insbesondere unter Berücksichtigung einer umfassenden Digitalisierung von allen Bereichen des täglichen Lebens, führt zu einem hohen Anspruch an die Sicherheit und die Verfügbarkeit von Telekommunikationsnetzen und -diensten.

Vor diesem Hintergrund definiert § 109 Telekommunikationsgesetz (TKG) bestimmte Schutzziele und Schutzpflichten. Als allgemeine Schutzziele bestimmt § 109 Abs. 1 TKG den Schutz personenbezogener Daten und den Schutz des Fernmeldegeheimnisses. Die Verfolgung dieser allgemeinen Schutzziele obliegt jedem Diensteanbieter. Die besonderen Schutzziele nach § 109 Abs. 2 TKG haben dagegen den Schutz der Telekommunikationsinfrastruktur vor Störungen und Risiken sowie die Verfügbarkeit der Telekommunikationsdienste zum Gegenstand. Die Verfolgung besonderer Schutzziele ist auf die Betreiber öffentlicher Telekommunikationsnetze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste eingeschränkt.

Zur Erreichung der Schutzziele haben alle Unternehmen technische Vorkehrungen und sonstige Maßnahmen zu treffen. Zur Verfolgung der besonderen Schutzziele sind insbesondere auch Maßnahmen zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe zu treffen, um Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Zur besseren Beherrschbarkeit der Risiken für Telekommunikationsinfrastruktur und Verfügbarkeit der Telekommunikationsdienste sieht § 109 Abs. 4 TKG die Erstellung von Sicherheitskonzepten und die Benennung von Sicherheitsbeauftragten vor.

Für staatliche Vorgaben gilt der Grundsatz der Verhältnismäßigkeit. Von den Unternehmen können daher nur geeignete, erforderliche und angemessene technische Vorkehrungen und sonstige Maßnahmen erwartet werden. Im Rahmen der Erforderlichkeit einer Vorkehrung oder Maßnahme ist der Stand der Technik zu berücksichtigen (§ 109 Abs. 1 S. 2 TKG; § 109 Abs. 2 S. 3 TKG). Angemessen ist eine Vorkehrung oder Maßnahme dann, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht (§ 109 Abs. 2 S. 5 TKG).

In Erfüllung seiner telekommunikationsrechtlichen Pflichten hat das Unternehmen ergänzend die allgemeinen datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der Datenschutz-Grundverordnung (DSGVO) zu beachten. Werden telekommunikationsrechtliche Pflichten aus § 109 TKG im Auftrag eines Verantwortlichen durch andere Personen oder Stellen erfüllt und hierbei Daten verarbeitet, so hat der nach § 109 TKG Verantwortliche für die Einhaltung der telekommunikationsrechtlichen Vorschriften Sorge zu tragen. Unberührt hiervon bleibt die unmittelbare datenschutzrechtliche Verantwortlichkeit der beauftragten Person oder Stelle nach allgemeinem Datenschutzrecht.

2 Funktion und grundlegender Inhalt des Katalogs von Sicherheitsanforderungen

Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste haben die von ihnen ergriffenen technischen und organisatorischen Schutzmaßnahmen in einem Sicherheitskonzept darzustellen gemäß § 109 Abs. 4 TKG. Grundlage für dieses Sicherheitskonzept und für die zu ergreifenden technischen Vorkehrungen und sonstigen Maßnahmen ist der „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG“, den die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für die Sicherheit in der Informationstechnik und dem/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt hat.

Grundlegende Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten sind in 3. Kapitel beschrieben. Die Erfüllung dieser Sicherheitsanforderungen ist für alle Unternehmen zwingend. Ein Überblick über die einschlägigen gesetzlichen Anforderungen des TKG (§§ 88 - 109) soll Kapitel 4 geben. Hinweise zur Erstellung eines Sicherheitskonzeptes finden sich in Kapitel 5. Anlage 1 beschreibt geeignete technische und organisatorische Maßnahmen zur Anforderungen an TK-Diensteerbringer mit IP-Infrastruktur. Zusätzliche Sicherheitsanforderungen enthält die Anlage 2. Die zusätzlichen Sicherheitsanforderungen richten sich an Betreiber von Telekommunikationsnetzen mit erhöhtem Gefährdungspotential.

Die Verantwortung der richtigen und ordnungsgemäßen Umsetzung von Schutzmaßnahmen obliegt stets dem Verpflichteten. Er muss dafür Sorge tragen, dass auch bei einer Aufgabenübertragung an Dritte kein Sicherheitsverlust zu erwarten ist.

Die Bundesnetzagentur kann nach § 109 Abs. 7 TKG anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder einer zuständigen nationalen Behörde unterziehen. Eine solche Überprüfung soll feststellen, ob die Anforderungen nach § 109 Abs. 1 bis 3 TKG erfüllt sind. Der Katalog für Sicherheitsanforderungen kann somit auch Grundlage für das Sicherheitsaudit einer qualifizierten unabhängigen Stelle nach § 109 Abs. 7 TKG sein.

In die Erstellung des Kataloges wurden Hersteller, Verbände der Betreiber öffentlicher Telekommunikationsnetze und Verbände der Anbieter öffentlich zugänglicher Telekommunikationsdienste eingebunden.

3 Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten

Ein ganzheitliches Konzept bildet die Basis und den Ausgangspunkt zum Aufbau eines tragfähigen Sicherheitsmanagements. Informationssicherheitsmanagement, oder kurz IS-Management, ist der Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll. Informationssicherheit ist aber nicht nur eine Frage der Technik. Um ein bedarfsgerechtes Sicherheitsniveau für alle Geschäftsprozesse, Informationen und der Technik zu erreichen, sind in erheblichem Maße auch geeignete organisatorische und personelle Rahmenbedingungen zu schaffen.

Die im Folgenden aufgelisteten Sicherheitsanforderungen greifen diese Aspekte auf. Die Anforderungen gelten für alle pflichtigen Unternehmen und sind allgemeiner Natur. Sie bilden insofern die Grundlage für alle umzusetzenden Schutzmaßnahmen. Die aus den Sicherheitsanforderungen abgeleiteten Schutzmaßnahmen müssen im Weiteren angemessen in dem zu erstellenden Sicherheitskonzept berücksichtigt werden. Die Beurteilung der Angemessenheit einer sicherheitskonzeptionellen Schutzmaßnahme liegt hierbei zunächst in der Eigenverantwortung des pflichtigen Unternehmens. Dabei handelt es sich um einen kontinuierlichen Beurteilungsprozess, bei dem Strategien und Maßnahmen stetig überprüft und an veränderte Anforderungen angepasst werden. Die Bundesnetzagentur überprüft regelmäßig die Einhaltung der Vorgaben des Sicherheitskatalogs und die Umsetzung des Sicherheitskonzepts.

Auch die Sicherheitsanforderungen des vorliegenden Kataloges sind daher weder abschließend, noch zeitlich unveränderlich. Je nach Kritikalität eines bestimmten Netzes oder Dienstes bzw. Entwicklung der Technik sind im Einzelfall weitergehende Anforderungen erforderlich.

3.1 Organisation

Handelt es sich bei dem pflichtigen Unternehmen um einen Kaufmann oder eine Einpersonengesellschaft, so sind die Verantwortlichkeiten und Prozesse einfach zuzuordnen. In vielen Fällen fußt die Pflicht aus § 109 Abs. 1 bis 3 TKG jedoch auf einem arbeitsteiligen

Betrieb oder Angebot. Die Leitungsperson eines pflichtigen arbeitsteiligen Unternehmens hat daher auf eine eindeutige und festgelegte Aufbau- und Ablauforganisation zu achten. Hierzu gehört auch die Benennung des Sicherheitsbeauftragten nach § 109 Abs. 4 TKG.

3.1.1 Organisations- und Risikomanagement

Jedes Unternehmen hat sicherzustellen, dass ein verbindliches Verfahren festgelegt ist, um Risiken für Netzwerke, Dienste und die Verarbeitung personenbezogener Daten zu erkennen. Identifizierte, wesentliche Gefährdungen (Sicherheitsrisiken) für Netze, Dienste und Daten sind zu dokumentieren Erkannte Restrisiken sollen unter Berücksichtigung der Verhältnismäßigkeit kontrolliert werden.

3.1.2 Sicherheitsrollen und Verantwortlichkeiten

Für die Sicherheit von Informationen, Geschäftsprozessen, Anwendungen, Aufgaben und Regelungen ist eine personelle Verantwortlichkeit festzulegen. Es sind alle Mitarbeiter über diese Verantwortlichkeiten in geeigneter Weise zu informieren. Es soll ein Hinweis ergehen, wann und wie die für Sicherheit Zuständigen zu beteiligen sind.

- Bei der Vergabe der jeweiligen Sicherheitsrollen kann ein Ernennungsakt Klarheit, Transparenz und Öffentlichkeit verschaffen. In diesem Zusammenhang könnte auch eine Festlegung von Aufgaben und Befugnissen erfolgen.
- Benennung alleine ist nicht ausreichend. Die für Sicherheitsvorfälle zuständigen Personen müssen in der Wahrnehmung ihrer Rollen erreichbar sein. Die Schaffung einer Vertretungsregelung ist in diesem Zusammenhang eine wichtige Voraussetzung.
- Sicherheitskenntnisse altern. Es soll daher eine regelmäßige Schulung des benannten Personals durchgeführt werden.

3.1.3 Lieferantenmanagement

Die Bereitstellung von Telekommunikationsdiensten kann oft nur unter Rückgriff auf Dritte erfolgen. Lieferanten und Erfüllungsgehilfen nehmen vor diesem Hintergrund eine wichtige Rolle ein. Das pflichtige Unternehmen muss daher eine Bewertung der Zuverlässigkeit, Vertrauenswürdigkeit und Qualität des Erfüllungsgehilfen oder Lieferanten vornehmen. Es ist sicherzustellen, dass durch die Abhängigkeiten von Dritten die Sicherheit von Netzwerken oder Dienstleistungen sowie personenbezogener Daten nicht beeinträchtigt wird. In diesem Zusammenhang ist auf Folgendes zu achten:

- Eine Bewertung der Zuverlässigkeit des Dritten ist nur auf der Grundlage von geeigneten Informationen möglich. Daher gilt: Informationseinholung hat vor Beauftragung zu erfolgen.
- Dritte sind vertraglich zu binden. Es ist hierbei sicherzustellen, dass Sicherheitsanforderungen in die vertragliche Grundlage mit Anbietern einbezogen werden (z. B. beim Erwerb von IT-Produkten oder der Inanspruchnahme von IT-Services). Besondere Sorgfalt sollte in dieser Hinsicht gelten, sofern ganze Geschäftsprozesse (Helpdesks, Call Center, Netzwerkverbindungen) ausgelagert werden).
- Das datenschutzrechtlich konforme Handeln der Dritten ist sicherzustellen. Dies kann durch entsprechende vertragliche Regelungen erfolgen. Bei Auftragsverarbeitung sind die Regelungen des Art. 28 DSGVO zu beachten.
- Die Sicherheitsanforderungen sollten nicht nur festgelegt und aktualisiert, sondern auch in ihrer Einhaltung möglichst überprüft werden. Bei einer Auftragsverarbeitung muss dies grundsätzlich erfolgen. Die Überprüfungen sollten regelmäßig wiederholt werden.

3.2 Sicherheit im Personalmanagement

Mitarbeiter liefern einen wesentlichen Beitrag zur Einhaltung der eingangs erwähnten Schutzziele. Aufwendige Schutzmaßnahmen und technische Redundanzkonzepte bringen nur den gewünschten Erfolg, wenn auch die Mitarbeiter keine Sicherheitslücke im Unternehmen darstellen und der Verantwortung ihrer sicherheitsrelevanten Tätigkeit bewusst sind. Dieses Kapitel umfasst die Sicherheitsanforderungen an die Personalabteilung, die Geschäftsführung und das Personal im Unternehmen. Hierzu gehört auch Personal, welches zur Erledigung bestimmter Aufgaben extern bereitgestellt wird (z. B. von Lieferanten oder Herstellern).

Bereits vor der Einstellung und auch nach dem Verlassen des Unternehmens sind die nachfolgenden Anforderungen zu berücksichtigen.

3.2.1 Sicherheitsüberprüfung

Je nach Aufgabe und Verantwortlichkeit kann eine angemessene Sicherheitsüberprüfung erforderlich sein. Im Hinblick auf Mitarbeiter und Auftragnehmer ist es angezeigt, die Identität und die berufliche Referenz, vor allem bei Personen mit sicherheitsrelevanten Aufgaben und Verantwortlichkeiten (z. B. bei Systemadministratoren, Sicherheitsbeauftragten oder

Wachpersonal), zu validieren. Die jeweils eingesetzte Prüfungsmodalität sollte dokumentiert werden.
Zur eindeutigen Feststellung der Identität sollte das Unternehmen Mitarbeiter zur Vorlage des Personalausweises auffordern. Weitere geeignete Nachweise können beglaubigte Zeugniskopien, Personenzertifikate oder eines amtlichen Führungszeugnisses sein. Es bietet sich u.U. an, weitere zusätzliche Referenzen von früheren Arbeitgebern einzuholen.

3.2.2 Sicherheitswissen und Sensibilisierung

Das Personal muss über geeignete und relevante Sicherheitskenntnisse verfügen und ein Bewusstsein für den Umgang mit sensiblen Daten entwickeln.

Es ist daher sicherzustellen, dass das eingesetzte und beauftragte Personal geeignete und relevante Schulungen besucht hat und Material zu Sicherheitsfragen zur Verfügung gestellt wird. Der Besuch der Schulung ist zu dokumentieren.

Wissen altert. Es sollten daher regelmäßige Schulungsmaßnahmen und Sensibilisierungssitzungen für eingesetztes und beauftragtes Personal zu den betreffenden Sicherheitsthemen (z.B. Datenschutz, Fernmeldegeheimnis) abgehalten werden.

Auch Schulungsinhalte sollten regelmäßig unter Berücksichtigung von Änderungen überprüft und ggf. aktualisiert werden.

3.2.3 Personelle Veränderungen

Ein Personalwechsel ist mit Sicherheitsrisiken verbunden. Wenn Mitarbeiter den Aufgabenbereich wechseln, das Unternehmen verlassen oder neue Mitarbeiter eingearbeitet werden, muss daher das Unternehmen bestimmte Sicherheitsanforderungen beachten:

- Es sind Regelungen für die Verwaltung von Personalveränderungen oder Änderungen von Zuständigkeiten und Verantwortlichkeiten zu wahren.
- Nach einem Personal- oder Beauftragtenwechsel sind Zugriffs, Zutritts- und Zugangsrechte zu entsprechenden Systemen, Gebäuden oder Anlagen unverzüglich anzupassen bzw. zu sperren. Ausgegebene Passwörter sind nach dem Stand der Technik zu verwalten.
- Neues Personal muss über geltende Richtlinien und Verfahren informiert und sensibilisiert werden.

3.2.4 Umgang mit Verstößen

Es sollten verbindliche Regelungen festgelegt werden, wie mit Sicherheitsverletzungen aufgrund von Verstößen durch eigene Mitarbeiter umgegangen wird.

3.3 Sicherheit von Daten, Systemen und Einrichtungen

Dieses Kapitel umfasst die physische und logische Sicherheit von Daten, Netzwerk- und Informationssystemen zum Schutz der Grundwerte (Vertraulichkeit, Verfügbarkeit und Integrität).

3.3.1 Sicherer Umgang mit sensiblen Daten und Informationen

Im Bereich der Telekommunikation ist der Schutz von Bestands- und vor allem der von hoch sensiblen Daten, wie z.B. Verkehrs-, Steuer- oder Inhaltsdaten zu gewährleisten. Sie unterliegen dem Datenschutz und dem Schutz des Fernmeldegeheimnisses. Es müssen daher Regelungen zum sicheren Umgang mit solchen Daten und Informationen getroffen werden. Insbesondere gilt:

- Sensible Akten oder Dokumente müssen unter Verschluss verwahrt werden. Abschließbare Aktenschränke, verschlossene Büroräume sollten als mögliche Maßnahmen berücksichtigt werden.
- Mobile Endgeräte oder Wechseldatenträger sollten mit geeigneten Verschlüsselungstechnologien geschützt werden. Es sollte ein (MDM) Mobile Device Management genutzt werden.
- Es sollten Regelungen zur sicheren Entsorgung von Wechseldatenträgern, die nicht mehr benötigt werden oder defekt sind, getroffen werden.
- Festplatten mit sensiblen Daten müssen so entsorgt werden, dass eine Wiederherstellung der Daten nicht mehr möglich ist.

3.3.2 Physische und elementare Schutzanforderungen

Ein Sicherheitsrisiko besteht auch durch Vandalismus, Diebstahl, Feuer, Wasser, Staub oder Elementarschäden. Durch geeignete physische Schutzmaßnahmen sollten Sicherheitsrisiken dieser Art möglichst abgewehrt werden, damit die Verfügbarkeit von Netz und Dienst gewahrt bleibt. Dies beinhaltet mindestens die folgenden Maßnahmen:

- Es sind physische Sicherheitselemente festzulegen, die den unbefugten Zutritt, die Beschädigung und die Beeinträchtigung von Informationen und informationsverarbeitenden Einrichtungen verhindern (z.B. durch

Sicherheitsschlösser, Bewegungsmelder, Einbruchmeldeanlagen oder Videoüberwachung).

- Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung geschützt werden.
- Geräte und Betriebsmittel sind in regelmäßigen oder durch den Hersteller empfohlenen Intervallen zu warten.
- Telekommunikationsverkabelung und Stromverkabelung sind vor Unterbrechung, Störung und Beschädigung angemessen zu schützen. Redundante Leitungen sind voneinander getrennt zu verlegen. Kabel sollten unterirdisch verlegt werden und durch Rohre und verschlossene Räume und Schränke geschützt werden.
- Wasserführende Leitungen sollten in Serverräumen vermieden werden.
- Maßnahmen zum Schutz vor Naturkatastrophen und Unfällen sind zu ergreifen.
- Es ist eine regelmäßige Bewertung der Wirksamkeit von physischen und umgebungsbezogenen Schutzmaßnahmen vorzunehmen.
- Der Einsatz von Feuer-, Gas- und Rauchmeldern oder Löschanlagen sollte der Größe der Räumlichkeiten angemessen vorhanden sein und regelmäßig gewartet werden.
- Die Einhaltung der Brandschutzordnung muss regelmäßig überprüft werden.

3.3.3 Versorgungssicherheit (Verfügbarkeit des Gesamtsystems)

Ein wichtiger Bestandteil im Bereich der öffentlich zugänglichen Telekommunikation ist die Gewährleistung der Versorgungssicherheit (Telekommunikation, Elektrizität, Klimatisierung, usw.). Folgende Schutzmaßnahmen sind zu ergreifen:

- Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen zu schützen.
- Es sollten redundante Leitungen über unterschiedliche Zuleitungswege vorhanden sein.
- Eine ausreichende Dimensionierung der Klimatisierung und Stromversorgung ist festzulegen und regelmäßig zu überwachen.
- Schaltanlagen, Notstromgeneratoren, Batterien, etc. müssen regelmäßig kontrolliert und falls möglich getestet werden.
- Ein Verfahren zur Umsetzung für die Sicherheit kritischer Versorgungsgüter, Versorgungseinrichtungen und unterstützenden Einrichtungen ist zu erstellen.
- Maßnahmen zum Schutz der Lieferung und Bereitstellung der Versorgungseinrichtungen sind zu implementieren.

3.3.4 Zugriffs- und Zugangskontrolle auf Netzwerk- und Informationssystemen

Ohne geeignete Mechanismen zur Zugriffs- und Zugangskontrolle kann eine unberechtigte Nutzung von TK-Geräten und TK-Systemen nicht verhindert werden. Unbefugte können auch an vertrauliche Informationen gelangen, Manipulationen vornehmen oder Störungen verursachen. Durch geeignete Berechtigungen soll der Zugang und der Zugriff auf Informationen kontrolliert und gesteuert werden.

Mögliche Schutzmaßnahmen sind:

- Nutzer haben eindeutige Kennungen und werden authentifiziert, bevor sie auf Dienste oder Systeme zugreifen dürfen.
- Passwörter dürfen nur verschlüsselt gespeichert werden.
- Rollen, Rechte, Verantwortlichkeiten und Verfahren zum Zuweisen und Widerrufen von Zugriffsrechten sind festzulegen.
- Zugriffe auf Netzwerk- und Informationssysteme müssen protokolliert werden. Abweichungen von dieser Verfahrensweise müssen hinterlegt und protokolliert werden.
- Fernwartungszugänge müssen ausreichend gesichert werden (eigene VPN-Zugänge).
- Fremde Personen dürfen sich nur in Begleitung oder nach geeigneter Sicherheitsüberprüfung und Einweisung in gesicherten Bereichen aufhalten. Fremde Personen sind hierbei Personen von externen Firmen z.B. bei Wartungsarbeiten, Umbauten oder auch Reinigungsarbeiten.
- Die Zugangskontrollmechanismen werden regelmäßig überprüft und bei Bedarf angepasst.
- Für gesicherte technische Anlagen muss sichergestellt sein, dass nur Personen mit Befugnis Zugriff haben.

3.3.5 Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen

Die Integrität und Verfügbarkeit von Netzwerk- und Informationssystemen und der Schutz vor Viren, Code-Injektionen und anderer Malware, die die Funktionalität von Systemen verändern kann, ist zu gewährleisten:

- Es ist sicherzustellen, dass Software von Netzwerk- und Informationssystemen nicht unberechtigt manipuliert oder verändert wird (z.B. durch nicht-autorisierte Änderung der Konfiguration). Änderungen sollten dokumentiert werden. Unberechtigte Zugriffe

müssen detektiert werden. Systeme und Anwendungen sollten immer die aktuellen Sicherheitsupdates erhalten.

- Es müssen geeignete Maßnahmen zur Erkennung von Schadsoftware umgesetzt werden.
- Maßnahmen zur Sensibilisierung der Mitarbeiter sollen bestehen und umgesetzt werden.
- Es ist sicherzustellen, dass sicherheitskritische Daten (wie Passwörter, gemeinsame geheime Schlüssel, private Schlüssel usw.) nicht offengelegt oder manipuliert werden.
- Die Wirksamkeit der Maßnahmen zum Schutz der Integrität von Systemen sollte überprüft und bewertet werden.
- Passwörter sollten sicher authentifiziert und bei Bedarf geändert werden.
- Mitarbeiter sollten durch Schulungsmaßnahmen befähigt sein, verdächtige E-Mails oder Links zu erkennen.

3.3.6 Vertraulichkeit der Kommunikation

Die Vertraulichkeit und die Integrität von Kommunikationsinhalten und Metadaten sind zu gewährleisten:

- Zur Sicherstellung eines angemessenen Schutzes der Vertraulichkeit von Kommunikationsinhalten und Metadaten sollten geeignete Verschlüsselungsverfahren eingesetzt werden.
- Es sind geeignete Authentifizierungsmechanismen für Kunden- und Dienstleistungsnetzwerke zu implementieren.
- Die Nutzung von Netzwerken und Diensten sollte fortwährend in geeigneter Form auf Anomalien sondiert werden.
- Es sollten standardisierte Übertragungsverfahren und -maßnahmen verwendet werden.
- Sicherheitskritische Daten von Kunden sind besonders zu schützen (z.B. Daten der SIM-Karten, IMEI-Nummer, Passwörter).
- Auch die Wirksamkeit von Methoden zum Schutz der Vertraulichkeit von Kommunikationsinhalten und -metadaten sollte stetig in geeigneter Form bewertet werden. Standortdaten wie beispielsweise Cell-IDs gehören ebenfalls zu den Metadaten und unterliegen zusätzlichen Anforderungen (siehe Abschnitt 4.2.4). Eine geeignete Bewertung kann die Ausführung einer Gegenprüfung (Cross-Checks) oder die Durchführung eines (Stress)Tests sein.

3.4 Betriebsführung

Die verantwortliche Unternehmensführung hat den ordnungsgemäßen und sicheren Betrieb zu gewährleisten. Die nachfolgenden Sicherheitsanforderungen haben das operative Betriebsverfahren, das Änderungsmanagement und den Umgang mit Unternehmenswerten zum Gegenstand.

3.4.1 Betriebsverfahren

Durch geeignete Betriebsverfahren ist sicherzustellen, dass die Informations- und Kommunikationstechnologie des jeweiligen pflichtigen Unternehmens ordnungsgemäß, sicher und kontinuierlich funktioniert.

- Um dies sicherstellen zu können, muss im Mindestmaß der Betriebsablauf festgelegt und dokumentiert werden. Ferner müssen die Verantwortlichkeiten für den Betrieb kritischer Systeme einer zuständigen Stelle zugewiesen sein.

- Verfügbare und notwendige Ressourcen müssen bekannt sein. Ressourcen in diesem Sinn umfassen u.a. das notwendige und tatsächliche Personal, Systeme, Anwendungen und Räumlichkeiten.
- Verfügbare und notwendige Ressourcen müssen stetig überprüft und ggf. in geeigneter Form gesteuert werden.

3.4.2 Änderungsmanagement

Veränderungen können Sicherheitsrisiken bergen. Sich schnell ändernde und stetig steigende Anforderungen der Benutzer führen beim pflichtigen Unternehmen zudem zu immer kürzeren Änderungsintervallen einschließlich Anpassungen von Systemkonfigurationen. Unternehmen können insofern vor der Aufgabe stehen, TK-Komponenten bedarfsgerecht und zeitnah, aber auch sicher aktualisieren zu müssen. Die Sicherheitspraxis zeigt, dass Risiken oder Betriebsstörungen häufig auf fehlerhaftes, übereiltes oder keinerlei geeignetes Änderungsmanagement zurückzuführen sind. Zur Vermeidung von Störungen oder Sicherheitsvorfällen sollten daher Änderungen an Netzwerk- und Informationssystemen, Infrastruktur, Dokumentationen, Prozessen, Verfahren und Betriebsabläufen geplant, kontrolliert, gesteuert und nach Abschluss überprüft werden.

- Änderungen an kritischen Systemen sollen auf der Grundlage von vordefinierten und in geeigneter Form dokumentierten Verfahren erfolgen.
- Es sollte eine Einschätzung aller potenziellen direkten und indirekten Auswirkungen vorgenommen werden.
- Wesentliche tatsächliche Änderungen sollten in geeigneter Form protokolliert werden.
- Die Funktionalität der TK-Systeme sollte nach Änderungen in geeigneter Form überprüft werden. Alle betroffenen Personen sollten über die erforderlichen Änderungsdetails informiert werden. Identifizierte Auffälligkeiten sollten sofort der vorher festgelegten Stelle angezeigt werden.
- Es empfehlen sich Maßnahmen der präventiven Kontrolle, z. B. das 4-Augenprinzip.

3.4.3 Asset Management

Sicherheit erfordert Kenntnis. Zumindest die wesentlichen Anlagen, Systeme und Einrichtungen, welche für den jeweiligen Netzbetrieb oder das Diensteangebot erforderlich sind, sollten eindeutig identifizierbar sein. Eine entsprechende Inventarisierung und Verwaltung von Anlagen und Systemen kann dies im Einzelfall sicherstellen. Die Verwaltung sollte auch die Konfigurationssteuerung der wesentlichen Netzwerk- und Kommunikationssysteme einschließen.

3.5 Störungen und Sicherheitsvorfälle

Behandelt werden das Erkennen, die Reaktion auf sowie die Meldung von Störungen und Sicherheitsvorfällen. Sicherheitsvorfälle können durch ein einzelnes Ereignis oder eine Verkettung verschiedener Umstände ausgelöst werden. Sicherheitsvorfälle können dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Authentizität von Informationen und TK-Systemen beeinträchtigt werden.

3.5.1 Erkennen von Sicherheitsvorfällen und Störungen

Es muss ein Verfahren zum Erkennen von Sicherheitsvorfällen und Störungen eingerichtet und regelmäßig kontrolliert werden.
Hierzu sind z.B. vordefinierte Betriebsparameter wie Klima, Strom, Datenaufkommen im TK-Verkehr zu überwachen und im Sicherheitsvorfall oder bei Störungen zu alarmieren.
Nach Bekanntwerden von Störungen und/oder Vorfällen sollten betroffene Systeme so angepasst und/oder verbessert werden, dass zukünftig diese Problematik verhindert wird.

3.5.2 Umgang mit Sicherheitsvorfällen und Störungen

Ein Sicherheitsvorfall kann einen singulären oder multikausalen Ursprung haben. Jede Art von Sicherheitsvorfall kann dazu führen, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und TK-Systemen beeinträchtigt wird. Die pflichtigen Unternehmen haben daher ein Verfahren zur Definition und zum Umgang mit jedweder Art von Sicherheitsvorfall, einschließlich dessen Meldung an zuständige Personen und Behörden zu implementieren. Es sollte regelmäßig überprüft werden, ob das festgelegte Verfahren den aktuellen Umständen entspricht und die tatsächliche Umsetzung planungskonform erfolgt.

- Für Sicherheitsvorfälle hat geeignetes Personal verfügbar und benannt zu sein. Im Falle einer Sicherheitsverletzung kann es notwendig sein, unter Zeitdruck oder atypischen Umständen Sicherheitshandlungen durchzuführen oder sicherheitsrelevante Entscheidungen zu treffen. Das Personal sollte daher nicht nur für die Identifizierung, sondern auch für den speziellen Umgang mit Sicherheitsvorfällen geschult sein.
- Die Kritikalität der jeweiligen Störung oder Sicherheitsverletzung muss in geeigneter Form bewertet werden. Der für das Bewertungsergebnis vorgegebene Meldeweg muss sodann umgesetzt werden.
- Kritische Sicherheitsvorfälle müssen grundsätzlich untersucht werden. Untersuchung und Ergebnis muss in einem Bericht dokumentiert werden. Aus dem Bericht sollte

hervorgehen, welche Maßnahmen getroffen oder geplant sind, um gleichgelagerte Sicherheitsvorfälle und deren Auswirkungen zukünftig zu vermeiden oder das Sicherheitsrisiko zu minimieren. Die in dieser Hinsicht getroffenen oder geplanten Maßnahmen sollten begründet werden. Handelt es sich um beträchtliche Sicherheitsverletzungen gemäß § 109 Abs. 5 TKG, sind diese unverzüglich der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik mitzuteilen.

3.5.3 Kommunikation und Meldung von Sicherheitsvorfällen

Um den Schaden bei Sicherheitsvorfällen so gering wie möglich zu halten, sollten angemessene Verfahren zur Meldung von Sicherheitsereignissen vorhanden sein.

- Ein Sicherheitsvorfall kann eine gesetzliche Meldepflicht (z. B. §§109 Abs. 5, 109a Abs. 1 TKG oder Art. 33 DSGVO) auslösen. Falls erforderlich sind daher Meldungen über aktuelle oder zurückliegende Sicherheitsereignisse an Dritte, Kunden und/ oder Behörden durchzuführen.
- Zur Sicherstellung etwaiger Meldepflichten sowie der Kommunikation und Berichterstattung von Sicherheitsvorfällen sollten geeignete Regelungen in die unternehmerischen Betriebsabläufe implementiert werden.
- Bei einem Angriff auf Passwörter sind betroffene Kunden schnellstmöglich zu informieren. Zur Sicherstellung sollte ein geeignetes Meldeverfahren festgelegt werden.

3.6 Not- oder Ausfallmanagement

Eine Störung oder ein Sicherheitsvorfall kann zum Ausfall des Dienstes oder des Netzbetriebes führen. Eine geeignete Präventionsstrategie sollte Entwicklungen dieser Art berücksichtigen und entsprechende auf den Einzelfall angepasste Abwehrkonzepte entwickeln. In diesem Zusammenhang sind nicht nur die technischen Aspekte für die Aufrechterhaltung der Dienste zu regeln. Auch organisatorische Maßnahmen sind im Vorfeld zu planen, festzulegen und fortwährend zu überprüfen. Dieses Kapitel umfasst Anforderungen zur Wiederherstellung und Aufrechterhaltung betriebsrelevanter Infrastrukturen.

3.6.1 Aufrechterhaltung von Telekommunikationsinfrastrukturen und Diensten (Business Continuity Management)

Regelungen zur Aufrechterhaltung der Infrastrukturen und Dienste haben allgemeine Handlungsanweisungen und möglichst auch konkrete, auf den Einzelfall angepasste Notallmaßnahmen zu enthalten. Relevante Kontaktinformationen sollten in einem Notfallhandbuch beschrieben und stets aktuell sein. Der Zugriff auf diese Regelungen und Informationen sollte sichergestellt sein.

- Im Vorfeld ist die Verfügbarkeit angemessener Redundanzen auf System- und Dienstebene sicherzustellen.
- Diese Redundanzen sind in regelmäßigen Abständen zu testen bzw. umzuschalten, sofern dies unterbrechungsfrei möglich ist.
- Es sind regelmäßige Backups von kritischen Systemen und Daten zu erstellen. Auf die gesetzlich vorgegebenen Lösch- und Speicherfristen ist hierbei zu achten, insbesondere sollte die Speicherdauer der Backups in einem angemessenen Verhältnis zur Speicherdauer der personenbezogenen Daten stehen.
- Es sind angepasste Notfallpläne zum Betrieb kritischer Systeme auszuarbeiten, festzulegen und zu implementieren. Es sollte regelmäßig eine Evaluierung dieser Pläne erfolgen.
- Ein geeigneter Notfallbeauftragter ist zu benennen. Dieser sollte alle Aktivitäten des Notfallmanagements kennen und steuern.

3.6.2 Wiederanlauf nach Ausfällen (Disaster Recovery Management)

Die Ausfallzeiten bis zur Wiederherstellung der Funktionsfähigkeit von Netzwerk und Kommunikationsdiensten müssen dennoch mit angemessenen Mitteln so gering wie möglich gehalten werden.

- Es sind geeignete Richtlinien und Verfahren zur schnellstmöglichen Wiederherstellung wichtiger Netzwerk- und Kommunikationsdienste zu entwickeln und festzulegen. Diese Richtlinien und Verfahren sollten in regelmäßigen Abständen evaluiert werden.
- Die wichtigsten Geschäftsprozesse für den Wiederanlauf sollten priorisiert werden.
- Im Vorfeld sollten Lieferantenverträge auf eine Ersatzbereitstellung geprüft werden.
- Eine geeignete Schutzmaßnahme kann die Vorhaltung geeigneter Ersatzgeräte für Infrastruktur und TK-Systeme sein.
- Eine geeignete Schutzmaßnahme kann im Einzelfall auch die Vorhaltung geeigneter, mobiler Netzersatzanlagen sein.

- Zur Aufrechterhaltung von Dienstleistungen kann die präventive Einrichtung von Notfallarbeitsplätzen für Mitarbeiter sinnvoll sein.

3.7 Überwachungs- und Testverfahren

Um Systeme und Prozesse möglichst sicher zu gestalten und stets zu optimieren, sollten Überwachungs- und Testverfahren eingeführt werden. Nachfolgend werden Anforderungen zur Überwachung und Protokollierung wichtiger Netzwerk- und Kommunikationssysteme beschrieben.

3.7.1 Überwachungs- und Protokollierungsmaßnahmen

Geschäfts- und sicherheitsrelevante Ereignisse sollten protokolliert werden. Protokollierungsdaten dienen der Auswertung und Überwachung bestimmter Ereignisse. Eine detailreiche und fortlaufende, möglichst automatische Protokollierung kann die Auswertungsmöglichkeiten erhöhen. Im günstigsten Fall lassen die Protokollierungsdaten auf der Grundlage einer forensischen Untersuchung eine geeignete Sicherheitsanalyse zu. Alle sicherheitsrelevanten Ereignisse sind daher zu protokollieren und in einer auswertbaren Form abzuspeichern. Werden Daten für diese Zwecke nicht mehr benötigt, so sind sie unverzüglich zu löschen.

- Es sollte ein auf den Einzelfall angepasstes Regelwerk für die Überwachung und Protokollierung betriebsrelevanter Systeme eingeführt und umgesetzt werden. Das Regelwerk sollte regelmäßig evaluiert werden.
- Durch die automatische Überwachung und Protokollierung betriebsrelevanter Systeme können im Einzelfall möglicherweise weitere, zur Auswertung geeignete Informationen gewonnen werden.
- Administrative Tätigkeiten oder Arbeiten an betriebsrelevanten Systemen sollten protokolliert werden.

3.7.2 Notfallübungen

Im Kapitel 3.6 wurden Anforderungen zur Aufrechterhaltung und zum Wiederanlauf von Infrastrukturen und Diensten nach Notfällen behandelt. Damit Notfallpläne und Verfahren unter Stresssituationen wie geplant umgesetzt werden können, sollten regelmäßig Notfallübungen durchgeführt werden. Daher sollte eine Vorgehensweise zum Testen und Üben von Notfallplänen zur Aufrechterhaltung und Wiederherstellung kritischer Dienste und

Infrastrukturen festlegt werden. Falls möglich und notwendig, sollte dies auch in Zusammenarbeit mit Dritten erfolgen.
Es sollen möglichst realistische und unterschiedliche Szenarien berücksichtigt werden. Festgestellt werden soll, ob geplante Ausfallzeiten nicht überschritten werden und ob die bestimmte Krisenleitung in der Praxis ihre Aufgaben erfüllt.

3.7.3 Testen von Netzwerk- und IT-Systemen

Änderungen oder Entwicklungsarbeiten an bestehenden Netzwerk- oder IT-Systemen sind mögliche Risikofaktoren. Es sollten daher schon im Vorfeld Regelungen zur Freigabe und zum Testen von Netzwerk- und IT-Systemen festgelegt werden.

- Netzwerk- oder IT-Systeme sollten auf gesonderten Testumgebungen getestet werden, bevor sie verwendet oder mit vorhandenen Systemen verbunden werden. Gleiches sollte auch bei Anpassungen oder z.B. nach Updates geschehen.
- Betriebsrelevante Systeme sollten regelmäßigen Sicherheitstests unterzogen werden. Dies gilt insbesondere dann, wenn neue Systeme eingeführt und Änderungen vorgenommen werden.
- Es muss sichergestellt sein, dass Tests keine Auswirkungen auf die Sicherheit von Netzwerken und Diensten haben. Die Verwendung von sensiblen Daten muss vermieden werden.

3.8 Beurteilung der Sicherheitsmaßnahmen

Alle Sicherheitsmaßnahmen müssen den Stand der Technik berücksichtigen. Die Technik entwickelt sich jedoch fortwährend weiter. Hiermit einhergehend unterliegt auch die Bedrohungslage einer ständigen Veränderung. Vor diesem Hintergrund müssen auch die getroffenen Sicherheitsmaßnahmen regelmäßig neu vom pflichtigen Unternehmen beurteilt werden. Daher sollte eine angemessene Strategie zur Beurteilung der im Einzelfall getroffenen Sicherheitsmaßnahmen erstellt werden.

- Es sollten im Mindestmaß Regelungen zur Beurteilung der getroffenen Schutzmaßnahmen erstellt werden.
- Regelmäßig durchgeführte Risikoanalysen sowie Erhebungen festgelegter Kennzahlen (z.B. Störungs- und Ausfallzeiten als Indikator) können für die Beurteilung der Sicherheitsmaßnahmen herangezogen werden.
- Durch regelmäßige und realistische Stresstests können möglicherweise neue Risikofaktoren identifiziert werden.

3.9 Einhaltung gesetzlicher Anforderungen

Die Einhaltung gesetzlicher, vertraglicher oder freiwilliger Regeln ist sicherzustellen. Hierzu sollte ein Überwachungssystem in die Betriebsabläufe implementiert werden und eine zuständige Stelle benannt werden. Auch das Recht unterliegt – ebenso wie die Technik oder die Bedrohungslage – einer fortwährenden Veränderung. Die Rechtsentwicklung sollte daher kontinuierlich und in geeigneter Form sondiert und deren Anwendung auf den Einzelfall geprüft werden. Eine Übersicht über einschlägige gesetzliche Regelungen des TKG gibt das nachfolgende Kapitel 4.

4 Rechtliche Sicherheitsanforderungen aus bereichsspezifischen Regelungen

Die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach § 109 Abs. 1 und 2 TKG zielen auf den Schutz personenbezogener Daten, das Fernmeldegeheimnis und den Schutz der Telekommunikationsinfrastruktur und der Verfügbarkeit von Diensten ab. Diese Rechtsgüter sind nicht ausschließlicher Regelungsgegenstand des TKG. Insofern sind vom pflichtigen Unternehmen u. U. auch andere europäische, verfassungsrechtliche oder nationale Vorschriften zu beachten.

Die nachfolgenden Ausführungen befassen sich ausschließlich mit den bereichsspezifischen rechtlichen Anforderungen des TKG. So finden sich Regelungen zum Schutz des Fernmeldegeheimnisses bereichsspezifisch in §§ 88 ff. TKG. Dem Schutz personenbezogener Daten obliegen die §§ 91 ff. TKG. Gegenstand der §§ 100, 109 Abs. 5 TKG ist der Schutz der Telekommunikationsinfrastruktur vor Störungen und die Verfügbarkeit der Telekommunikationsdienste.

Unionsrechtliche Vorgaben, sich verändernde Sicherheitslagen und technische Entwicklungen führen zu einer fortwährenden Novellierung des TKG. Die pflichtigen Unternehmen sind zur Wahrung ihrer gesetzlichen Pflichten daher grundsätzlich gehalten, den Verlauf der einschlägigen Gesetzgebung und Rechtsprechung zu beobachten und ihre Anwendung auf den Einzelfall zu prüfen. Insofern können die nachfolgenden Hinweise lediglich einen bereichsspezifischen und momentanen Überblick über einzuhaltende Anforderungen darstellen.

4.1 Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses (§ 88 TKG)

§ 88 TKG stellt die einfachrechtliche Ausprägung des verfassungsrechtlich verankerten Schutzes des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG dar. Das Gesetz trägt dem Umstand Rechnung, dass mit Liberalisierung des Telekommunikationsmarktes Telekommunikationsdienstleistungen durch Private erbracht werden und diese oftmals einer mittelbaren und damit nur relativen Grundrechtsbindung unterliegen. Vor diesem Hintergrund ergab sich die Notwendigkeit, den verfassungsrechtlichen Schutz aus Art. 10 Abs. 1 GG um eine Regelung auf einfachrechtlicher Ebene zu ergänzen und so die privaten Anbieter

ebenso wie die unmittelbar an Art. 10 Abs. 1 GG gebundenen staatlichen Stellen in die Pflicht zu nehmen.

Geschützt durch Art. 10 GG ist die Vertraulichkeit der Nutzung des zur Nachrichtenübermittlung eingesetzten technischen Mediums. Werden kommunikative Daten durch den Staat ohne Einwilligung zur Kenntnis genommen, aufgezeichnet, verwertet oder weitergegeben, so stellt dies ein Grundrechtseingriff dar. Wegen des Gleichklangs mit § 88 TKG verfolgt auch diese Vorschrift einen ähnlichen Inhalt. Im Unterschied zu Art. 10 GG entfaltet sich der Schutz jedoch nicht gegenüber dem Staat, sondern gegenüber den Diensteanbietern.
In Anlehnung an die verfassungsrechtliche Rechtsprechung zu Art. 10 Abs. 1 GG erfasst auch § 88 Abs. 1 TKG die näheren Umstände der Telekommunikation. Hierunter fallen alle Informationen über Zeit und Ort sowie Art und Weise des unkörperlichen Kommunikationsvorgangs, sofern diese eine Gefährdung der Vertraulichkeit des Kommunikationsvorgangs begründen können.

Im Hinblick auf die Einhaltung von Sicherheitsanforderungen zum Schutz des Fernmeldegeheimnisses soll auf folgendes hingewiesen werden:

- Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort.
- Es ist zu verhindern, dass Diensteanbieter sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen.
- Gleichermaßen ist zu verhindern, dass sich unbefugte Dritte Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation verschaffen.
- Zu berücksichtigen sind hierbei technische Einrichtungen zur mittelbaren und unmittelbaren Übertragung von Nachrichteninhalten, ferner auch Einrichtungen zur Erhebung, Verarbeitung und Nutzung von Verkehrsdaten (z.B. Teilnehmeranschluss, Netzabschlusspunkt, Vermittlungs- und Leitwegeinrichtungen, Verbindungsnetz sowie Billing- oder Fraud- Systeme).
- Im Bereich der Verwaltung und Verwahrung von Akten, welche dem Fernmeldegeheimnis unterliegen, sind für den Datenschutz hinreichend genügende Aufbewahrungsbehältnisse zu verwenden sowie entsprechende Räume mit Zutrittskontrolle sinnvoll einzusetzen.

- Es dürfen nur Personen Zugriff und Zugang haben, welche eine ausreichende Belehrung über die Sensibilität dieser Daten erhalten haben.
- Es muss sichergestellt werden, dass bei Nachrichtenübermittlungssystemen mit Zwischenspeicherung ausschließlich der Teilnehmer durch seine Einwilligung Inhalt, Umfang und Art der Verarbeitung bestimmt. Schutzmaßnahmen, die lediglich dem Teilnehmer selbst gestatten zu entscheiden, wer Nachrichteninhalte eingeben und darauf zugreifen darf, können durch entsprechende Zugangscodes und Kennwörter erfüllt werden. Diese werden nur dem Teilnehmer vertraulich übermittelt und sollen von diesem selbständig nach Erhalt verändert werden. Es liegt in der Einwilligungsfreiheit des Teilnehmers, an welche Person er die Zugangskennungen weitergibt.
- Schutzmaßnahme gegen eine ungerechtfertigte, entgegen dem Vertragsverhältnis vereinbarte Löschung von Nachrichteninhalten durch den Diensteanbieter kann beispielsweise das Anlegen von Backupsystemen sein.

4.2 Sicherheitsanforderungen zum Schutz der personenbezogenen Daten (§§ 91 ff. TKG)

Den bereichsspezifischen Datenschutz regelt der 2. Abschnitt des 7. Teils des TKG. Allgemeine datenschutzrechtliche Vorschriften der Datenschutz Grundverordnung (DSGVO) und die weiteren Regelungen des BDSG kommen ergänzend zur Anwendung.

Festgehalten werden kann, dass die DSGVO natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen dann keine zusätzlichen Pflichten auferlegt, wenn sie besonderen in der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) festgelegten Pflichten unterliegen, welche dasselbe Ziel verfolgen (Art. 95 DSGVO). Dementsprechend kommen Vorschriften der DSGVO vorrangig zur Anwendung, außer einer entgegenstehenden Regelung des TKG erfolgt in Umsetzung der ePrivacy-Richtlinie. § 95 TKG wird daher beispielsweise weitestgehend von der DSGVO verdrängt werden: Denn die ePrivacy-Richtlinie enthält – bis auf wenige Ausnahmen – keine Regelungen zur Verarbeitung von Bestandsdaten. Hiervon ausgenommen sind lediglich § 95 Abs. 2 S. 2 und 3 TKG als Umsetzung von Art. 13 Abs. 2 ePrivacy-Richtlinie. Auf entsprechende Ausführungen wurde daher im Folgenden verzichtet.