§ 165 TKG 2021 — Technische und organisatorische Schutzmaßnahmen

Telekommunikationsgesetz
Stand: 07.12.2025 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz des Fernmeldegeheimnisses und
2. gegen die Verletzung des Schutzes personenbezogener Daten.

Dabei ist der Stand der Technik zu berücksichtigen.

(2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und ?diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und
2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist unter Berücksichtigung des Stands der Technik, der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe des Betreibers oder des Anbieters sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

(2a) Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen nach Absatz 2 im Bereich der Sicherheit von Netzen und Diensten,
7. Grundlegende Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(2b) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2c) Geschäftsleitungen, die ihre Pflichten nach Absatz 2b verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(2d) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Nummer 41 des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.

(4) Kritische Komponenten im Sinne von § 2 Nummer 23 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.

(5) Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen.

(6) Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 62 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.

(7) Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die Verpflichtungen nach den Absätzen 1 bis 5 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

(8) Im Falle des Eintritts eines Sicherheitsvorfalls oder der Feststellung einer erheblichen Gefahr kann die Bundesnetzagentur Maßnahmen zur Behebung des Sicherheitsvorfalls oder zur Abwendung der Gefahr

und deren Umsetzungsfristen anordnen.

(9) Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 7 erfüllt sind. Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 7 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung fest. Der nach den Sätzen 1 und 2 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat, zu übermitteln. Er trägt die Kosten dieser Überprüfung. Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept nach § 166 erfolgt durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.

(10) Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.

(11) Die Bundesnetzagentur kann zur Unterstützung ein Computer-Notfallteam gemäß Artikel 10 der Richtlinie (EU) 2022/2555 im Rahmen der zugewiesenen Aufgaben in Anspruch nehmen. Die Bundesnetzagentur kann ferner das Bundesamt für Sicherheit in der Informationstechnik, die zuständigen nationalen Strafverfolgungsbehörden und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit konsultieren.