TTDSG[1]

Telekommunikation – Telemedien – Datenschutz - Gesetz (In Kraft ab 01.12.2021)

Wie das Bundesministerium für Wirtschaft und Energie zum Gesetzgebungsverfahren schreibt[2], werden hier die Bestimmungen zum Datenschutz aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) in einem Stammgesetz zusammengeführt. Es dient zum einen der Umsetzung der EU – Richtlinien (2002/58/EG, 2009/136/EG). Nachfolgend eine inhaltliche Kurzübersicht aus der „Datenschutzbrille“ mit einzelnen Ergänzungen.

Inhaltsverzeichnis (Kurzblick aus der "Datenschutzbrille")

1. Anwendungsbereich (Teil1)

i) Was?

Das TTDSG regelt den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und den Telemedien (Fernmeldegeheimnis, Abhörverbot, Geheimhaltungspflicht, Rufnummernunterdrückung, - anzeige, Anrufweiterschaltung, Weitergabe an und von Nutzerverzeichnissen, technisch - organisatorische Anforderungen, Auskunftspflichten, Speicherung, Weiterleitung, Transfer und Zugriff auf Endeinrichtungs- und Nutzerdaten).

ii) Wer?

Alle Unternehmen und Personen mit Sitz, Niederlassung, Dienstleistungs-, Informations- oder Warenangebot im Geltungsbereich, unabhängig ob eigenes oder fremdes Telemedienangebot, einschließlich der Mitwirkung daran oder des Zugangs dazu.

2. Telekommunikation (Teil2)

Teil 2 regelt die Vertraulichkeit der Kommunikation (§3, das Fernmeldegeheimnis),

i) § 4 Rechte der Erben und anderer, berechtigter Personen

Erben und anderer, berechtigter Personen können die Rechte des Endnutzer wahrnehmen.

Abhörverbot und Geheimhaltungspflicht (§5), Regelungen für die Zwischenspeicherung (§6),

ii) § 7 Vorlage amtlicher Ausweise

Nach dem TKG (§172) oder zur Prüfung der Angaben bei Vertragsabschluss, kann die Vorlage eines amtlichen Ausweises (auch elektronisch) verlangt werden. Es darf auch eine Kopie erstellt werden, allerdings ist nach Erfassung der für den Vertrag erforderlichen Angaben (und nicht mehr) diese unverzüglich zu vernichten. PS: Nach §20 Personalausweisgesetz[3], darf nur der Inhaber

1 Quelle: https://www.buzer.de/gesetz/14753/index.htm
2 Quelle: BMWi zum Gesetzgebungsverahren Netzpolitik (TTDSG)
3 Quelle: https://www.gesetze-im-internet.de/pauswg/__20.html

Kopien erstellen oder mit Zustimmung durch einen Dritten, wenn eindeutig als Kopie markiert! Bei Kopien empfiehlt das Bundesinnenministerium[4], alle Daten, die nicht der Identifizierung dienen, zu schwärzen. Dazu zählt die Dokumentnummer und die Zugangsnummer (CAN) zum automatisierten „Vor-Ort-Auslesen“ und nach zwei Fehlversuchen bei der Eingabe der Geheimzahl (PIN) erforderlich ist.

Missbrauch (§8),

iii) § 9 Verkehrsdaten

Es dürfen nur definierte Angaben gespeichert werden (Abs.1), die zur Aufrechterhaltung, der Entgeltabrechnung sowie zum weiteren Aufbau erforderlich sind. Danach sind diese unverzüglich zu löschen bzw. zu anonymisieren. Eine weitere oder zusätzliche Speicherung (z. B. für Werbezwecke) darf nur nach den Regeln der Datenschutz – Grundverordnung (DS-GVO) erfolgen.

Entgeltermittlung und Entgeltabrechnung (§10), Einzelverbindungsnachweis (§11), Störung und Missbrauch (§12),

iv) §13 Standortdaten

Auch diese dürfen – wenn - nur anonymisiert weiterverarbeitet werden, außer der Nutzer hat für definierte Zusatzdienste seine Einwilligung nach den Regeln der DS-GVO erteilt.

Information über ankommende Verbindungen (§14), grundsätzliches Angebot der Rufnummern-unterdrückung (§15) und der Weiterschaltung (§16), Endnutzerverzeichnisse (§17) und Endnutzer-datenbereitstellung (§18),

3. Telemedien und Endeinrichtungen (Teil3)

i) §19 Technische und organisatorische Vorkehrungen

Der Nutzer muss jederzeit die Möglichkeit haben, den angebotenen Dienst zu beenden und zwar ohne, dass Dritte Kenntnis davon erlangen. Soweit technisch möglich, ist eine anonyme oder pseudonymisierte Bezahlmöglichkeit zu schaffen und dem Nutzer anzuzeigen. Gleiches gilt für die Weiterleitung zu einem anderen Anbieter. Nach dem Stand der Technik (Verweis auf Verschlüsselung nach Anordnung des Bundesamtes für Sicherheit in der Informationstechnik, §7d BSI - Gesetz)[5] und wirtschaftlich zumutbar sind Vorkehrungen gegen unerlaubten Zugriff, Störungen und äußere Angriffe zu schaffen.

ii) §20 Daten Minderjähriger

dürfen nicht für kommerzielle Zwecke verwendet werden

iii) §§21 – 24 Bestandsdaten und der Umgang mit behördlichen Auskunftsverfahren

Bestandsdaten sind nach §2 Abs.(2) Nr.2 TTDSG schlicht: „Personenbezogene Daten“, dazu zählen explizit nicht Passwörter oder andere Zugriffsdaten. Auskunft darf im Einzelfall „auf Anordnung der zuständige Stelle“ (also Behörde) erteilt werden wenn sie erforderlich sind zur:

a) Durchsetzung der Rechte geistigen Eigentums
b) Durchsetzung zivilrechtlicher Ansprüche (auf gerichtliche Anordnung)
c) Verfolgung von Straftaten und Ordnungswidrigkeiten
d) Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung (Schutz der Freiheitsrechte, Leib und Leben, freiheitlich – demokratische Grundordnung, Allgemeingut u.s.w.)
   UND:
e) soweit zureichende, tatsächliche Anhaltspunkte vorliegen
   UND:
f) unter Angabe einer gesetzlichen Bestimmung verlangt werden.

Mit weiteren Regelungen (§22 Abs.3 Nr. 3 – 8) für Auskunftsersuchen des Bundeskriminalamtes (3), des Zollkriminalamtes /4) und der Landesbehörden (5), des Bundesverfassungsschutzes (6), dem Militärischen Abschirmdienst (7) und dem Bundesnachrichtendienst (8). Auskünfte über zugewiesene Internetprotokoll – Adressen sind gesondert (aber ähnlich) in §22 Abs.4 geregelt. Das

4 Quelle: Bundesministerium des Inneren, für Bau und Heimat: Ausweiskopien
5 Quelle: https://www.buzer.de/7d_BSIG.htm

Für den eiligen Leser kurz zusammengetragen (3/3)

Auskunftsersuchen ist durch eine Fachkraft zu prüfen und freizugeben. Gegenüber dem Betroffenen und Dritten ist Stillschweigen zu wahren (§22 Abs.5, 6).

UND WICHTIG:

g) Das Auskunftsersuchen ist unter Angabe einer gesetzlichen Bestimmung SCHRIFTLICH oder ELEKTRONISCH zu stellen. Bei Gefahr im Verzug ist diese umgehend nachzureichen (§24).

iv) §25 Schutz der Privatsphäre bei Endeinrichtungen

Die Speicherung und der Zugriff auf Endeinrichtung sind nur nach DS-GVO konformer Einwilligung *(z. B. Cookie)* und Verwaltung erlaubt. Ausnahmen: Nur auf dem lokalen Endgerät ohne Zugriff eines Dritten oder für die ausdrücklich gewünschte Nutzung erforderlich.

v) §26 Anerkannte Dienste zur Einwilligungsverwaltung & Endnutzereinstellungen

Für die Einwilligung ist ein nutzerfreundliches und wettbewerbskonformes (auch technisches) Verfahren einzusetzen, dabei darf kein wirtschaftliches Eigeninteresse vorliegen und die personenbezogenen Daten dürfen für keinen anderen Zweck verwendet werden. Dies ist mit einem Sicherheitskonzept (DS-GVO konform) zu dokumentieren und kann von einer unabhängigen Stelle* nach definierten Standards in §26 Abs.2 TTDSG anerkannt werden.

**) Hier sind wohl PIMS, Personal - Information - Management - Systeme gemeint (ggf. auch Single-Sign-On SSO) zur sicheren Verwaltung von personenbezogene Daten in lokalen oder Online - Speichersystemen[6]. Diese Systeme könnten / sollten von einer unabhängige Stelle auf Anerkennung geprüft sein, z. B. die TÜV – Gesellschaften.[7]*

4. Strafen, Bußgeld und Aufsicht (Teil4)

(a) §§27, 28 Straf- und Bußgeldvorschriften

Je nach Verfehlung sind Freiheitsstrafen bis zu zwei Jahren oder Geldstrafen bis zu € 300.000,00 möglich und die Bundesnetzagentur kann sogar ein Zwangsgeld bis zu € 1 Mio. verhängen.

(b) §§29, 30 Zuständige Behörden, Aufgaben und Befugnisse

Zuständige Behörden sind die Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und die Netzagentur (BNetzA). Für den BfDI gelten die Befugnisse nach Art.58 DS-GVO. Die BNetzA kann verpflichtend Auskünfte anfordern, Überprüfungen vornehmen, Geschäfts- und Betriebsräume betreten / besichtigen und ganz oder teilweise Dienste untersagen. Soweit zur Durchsetzung erforderlich, ist das Brief- und Postgeheimnis nach Art. 10 GG Abs.2 eingeschränkt.

5. Erkenntnisse zum Datenschutz?

Aus meiner Sicht, setzt das TTDSG konsequent die Regelungen der DS-GVO um. Die bisherige Lücke zur Regelung von behördlichen Auskunftsersuchen wird damit geschlossen. Die hier festgelegten Strafen sind auch nicht gerade „kleinlich“. In der EU befindet sich die ePrivacy – Verordnung zur Flankierung der DS-GVO und zur Ablösung der veralteten ePrivacy – Richtlinie unverändert in der Abstimmung. Weitere Regelungen zur Schnittstellenkommunikation, IoT, Wettbewerbsnutzung, Tracking, „End-to-End“ - Verschlüsselung u.ä. sind im Gespräch und deren Auswirkungen noch nicht absehbar.

Spannend ist das Thema „Personal – Information – Management – System“, als ein sicheres Kontroll- und Verwaltungssystem des einzelnen Individuums mit der Entscheidungsgewalt, wann und mit wem Daten geteilt oder nicht (mehr) geteilt werden. Ein solches System würde z. B. die „Cookie – Banner“ erübrigen.

Bei Bedarf zum Datenschutz, einfach einmal sprechen!

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

6 Quelle: European Data Protection Supvervisor zu PIMS
7 Quelle: ISO 27701 Zertifizierung – DEKRA | TÜV SÜD Zertifizierungen | TÜVIT Zertifizierungen