A1 Telekom Austria AG Richtlinie Datenschutz

Sichere Daten und transparente Regelungen

11.12.2023

öffentlich

Inhalt

Bei Personenbezeichnungen wird darauf geachtet, möglichst durchgängig eine gendergerechte Form zu verwenden (zum Beispiel Kund:innen, Mitarbeiter:innen). Aus Gründen der Lesbarkeit wird vereinzelt nur die männliche Form angeführt. Es sind aber stets Menschen sämtlicher Geschlechtskategorien gemeint.

Präambel

Sichere Daten und transparente Regelungen

Für ein Telekommunikationsunternehmen wie A1 Telekom Austria AG (in weiterer Folge „A1" genannt) ist es von besonderer Bedeutung, das Vertrauen der Kund:innen, Geschäftspartner:innen und Mitarbeiter:innen in den sicheren und sensiblen Umgang mit ihren Daten zu rechtfertigen.

Daher gelten für A1 unter diesem Aspekt drei Handlungsmaximen:

- Wir setzen rechtliche Regelungen zum Datenschutz konsequent um.
- Wir orientieren uns an den internationalen Standards der Datensicherheit.
- Unsere Regelungen bezüglich des Datenschutzes sind transparent.

Die in Artikel 5 DSGVO festgelegten Grundsätze sind Basis für unser Handeln. Die personenbezogenen Daten unserer Kunden:innen, Geschäftspartner:innen und Mitarbeiter:innen

☐ werden nur rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Art und Weise verarbeitet **(„Rechtmäßigkeit, Treu und Glauben, Transparenz")**;

☐ werden nur für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden **(„Zweckbindung")**;

☐ müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein **(„Datenminimierung")**;

☐ müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; im Hinblick auf die Zwecke ihrer Verarbeitung unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen **(„Richtigkeit")**;

☐ müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist **(„Speicherbegrenzung")**;

☐ werden in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet und sie vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen schützt **(„Integrität und Vertraulichkeit")**.

A1 als Verantwortlicher ist für die Einhaltung dieser Grundsätze verantwortlich und muss die Einhaltung nachweisen können **(„Rechenschaftspflicht")**.

1 Zielsetzung der Richtlinie

Die Achtung des Privat- und Familienlebens und der Schutz der Grundrechte und Grundfreiheiten ist A1 wichtig. Dies betrifft insbesondere den Umgang mit personenbezogenen Daten.

Kunden:innen, Geschäftspartner:innen und Mitarbeiter:innen vertrauen darauf, dass mit ihren Daten sorgfältig umgegangen wird. Dies beinhaltet das Ergreifen von geeigneten technischen und organisatorischen Maßnahmen, um personenbezogene Daten so zu verarbeiten, dass diese für unberechtigte Dritte nicht zugänglich und vor Zerstörung oder Verlust geschützt sind. Es ist Mitarbeiter:innen strikt untersagt, personenbezogene Daten, die ihnen im Rahmen ihres Dienstverhältnisses anvertraut oder zugänglich wurden, zweckwidrig zu nutzen oder sie unberechtigten Dritten zugänglich zu machen.

2 Geltungsbereich

Diese Richtlinie ist für alle Mitarbeiter:innen der A1 Telekom Austria AG verbindlich. Sie gilt für den Umgang mit allen personenbezogenen Daten, insbesondere Daten von Kund:innen, Geschäftspartner:innen und Mitarbeiter:innen.

3 Datenschutz und Datensicherheit

Die Begriffe Datenschutz und Datensicherheit handeln beide von der sicheren Verarbeitung von Daten. Obwohl eine klare Trennlinie schwer zu ziehen ist, beschreiben die beiden Worte unterschiedliche Aspekte, auf die nachfolgend kurz eingegangen werden soll.

Der **Datenschutz** behandelt in erster Linie den **juristischen Aspekt** der Datenverarbeitung. Dieser soll die **personenbezogenen Daten** eines Menschen und somit die Privatsphäre schützen. Dazu gibt es Gesetze und Vorschriften die genau festlegen, wie die Daten einer Person zu schützen sind - allen voran die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union sowie das österreichische Datenschutzgesetz (DSG). Beide Regelungen dienen dazu, dass Personen selbst bestimmen können was mit ihren Daten geschieht, die sie an Unternehmen und an diverse Einrichtungen bzw Behörden übermitteln.

Die **Datensicherheit** behandelt den **technischen Aspekt** der sicheren Verarbeitung jeglicher Art von Daten, also **personenbezogener und nicht personenbezogener Daten**. Dabei soll darauf geachtet werden, welche technischen und organisatorischen Maßnahmen erforderlich sind, um eine Datenmanipulation, Datenverlust oder den Zugriff unberechtigter Dritter auf Daten zu verhindern.

Um den rechtlichen Datenschutz zu gewährleisten bedarf es also unumgänglich der technischen und organisatorischen Datensicherheit.

4 Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn eine geeignete Rechtsgrundlage besteht. Eine solche kann insbesondere sein:

- Betroffene haben ihre Einwilligung erteilt.
- Die Verarbeitung der Daten ist für Zwecke vorvertraglicher Maßnahmen oder Vertragserfüllung erforderlich.

- Die Verarbeitung wird durch eine Rechtsvorschrift angeordnet oder erlaubt.
- Die Verarbeitung dient der Wahrung berechtigter Interessen, z.B. der Durchsetzung offener Forderungen. Dies gilt nicht, falls es einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen Betroffener das Interesse an der Verarbeitung überwiegen, insbesondere wenn es sich um Kinder handelt. Dies ist für jede Verarbeitung zu prüfen. Im Zweifel ist der oder die Datenschutzbeauftragte hierbei zu Rate zu ziehen.

Nur Mitarbeiter:innen, die explizit mit der Verarbeitung bestimmter personenbezogener Daten betraut wurden, sind hierzu im Rahmen der Erfüllung ihrer Aufgaben befugt.

5 Datenverarbeitung im Auftrag

Bei einer Datenverarbeitung durch Auftragsverarbeiter wird ein Dritter mit der Durchführung der Datenverarbeitung beauftragt, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Somit sind bei der Auftragserteilung folgende Maßnahmen zu befolgen:

Vor einer vertraglichen Vereinbarung ist zu überprüfen, ob der Auftragsverarbeiter die für die Verarbeitung notwendigen technischen und organisatorischen Anforderungen und Sicherheitsvorkehrungen gewährleisten kann.

Auftragsverarbeitungen dürfen nur auf Grundlage eines schriftlichen Vertrages erfolgen, in dem die Anforderungen an den Datenschutz, die Datensicherheit, das Telekommunikationsgeheimnis sowie die diesbezüglichen Kontrollrechte vereinbart sind und insbesondere festgehalten ist, dass die personenbezogenen Daten nur nach den Weisungen des Auftraggebers verarbeitet werden dürfen. A1 verwendet hierfür ein Muster einer Auftragsverarbeitervereinbarung, welches grundsätzlich zur Beauftragung von Auftragsverarbeitern heranzuziehen ist. Soll von diesem Muster abgewichen werden (z.B. weil der Auftragsverarbeiter sein eigenes Muster verwenden möchte oder Änderungen im Muster verlangt), ist dies in Abstimmung mit der Rechtsabteilung möglich.

Sollen die Daten außerhalb der Europäischen Union verarbeitet werden, muss der Auftragsverarbeiter ein der EU adäquates Datenschutzniveau garantieren. Zusätzlich sind die entsprechenden Bestimmungen der internen A1 Information Security Vorgaben zu beachten.

6 Übermittlung personenbezogener Daten

Die Weitergabe von personenbezogenen Daten an Dritte bedarf einer rechtlichen Grundlage (siehe Punkt 4). Vor der Weitergabe von Daten müssen angemessene Datenschutz- und Datensicherheitsmaßnahmen gewährleistet sein.

Konzerngesellschaften sind im Sinne des Datenschutzes als Dritte zu betrachten.

Die Übermittlung an staatliche Einrichtungen oder Behörden erfolgt ausschließlich aufgrund einschlägiger Rechtsvorschriften.

7 Rechte von Betroffenen

Betroffene haben hinsichtlich ihrer personenbezogenen Daten folgende Rechte:

Es besteht das Recht vom Verantwortlichen **Auskunft** zu verlangen, insbesondere:

- über die zu ihrer Person verarbeiteten Daten, inkl. ihrer Herkunft;
- über den Zweck der Verarbeitung;
- an wen die Daten übermittelt wurden;
- über die Dauer der Speicherung.

Es besteht ein Recht auf **Richtigstellung** der Daten, falls sie unrichtig oder unvollständig sind.

Es besteht ein Recht auf **Löschung** der Daten, falls die Datenverarbeitung unzulässig war oder die Daten für den Zweck der Datenverarbeitung nicht mehr erforderlich sind. Alternativ besteht ein Recht auf **Einschränkung** der Verarbeitung. Aufbewahrungspflichten müssen beachtet werden.

Es besteht ein **grundsätzliches Widerspruchsrecht** gegen die Verarbeitung der Daten, das zu berücksichtigen ist, wenn ein schutzwürdiges Interesse Betroffener aufgrund einer besonderen persönlichen Situation das Interesse des Verantwortlichen an der Verarbeitung überwiegt. Das gilt nicht, wenn eine Rechtsvorschrift den Verantwortlichen zur Durchführung der Verarbeitung verpflichtet.

Es besteht ein Recht auf **Datenübertragbarkeit**, aufgrund dessen Betroffene ohne Hindernis die Daten, die sie einem Verantwortlichen bereitgestellt haben, zu einem anderen Verantwortlichen mitnehmen können.

Betroffene dürfen wegen der Inanspruchnahme der hier beschriebenen Rechte nicht benachteiligt werden.

8 Weitere Prinzipien für die Verarbeitung personenbezogener Daten

Die nachfolgenden Prinzipien des Datenschutzes sind unverzichtbare Grundlage aller Datenanwendungen und Dienstleistungen in der A1:

Kommunikationsgeheimnis[1]

Das Kommunikationsgeheimnis schützt Inhalts-, Verkehrs- und Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche. Insbesondere ist das Abhören und Aufzeichnen von Kommunikationsinhalten verboten, außer es liegt eine Einwilligung aller Beteiligten vor oder es besteht eine gesetzliche Verpflichtung.

Alle Mitarbeiter:innen sowie Dritte, die für die A1 Telekom Austria AG tätig sind, sind zur Einhaltung des Kommunikationsgeheimnisses verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort.

[1] § 161 Telekommunikationsgesetz 2021 – TKG 2021

Datengeheimnis[2]

Verantwortliche, Auftragsverarbeiter und ihre Mitarbeiter:innen müssen personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht.

Mitarbeiter:innen dürfen personenbezogene Daten nur aufgrund einer ausdrücklichen Anordnung ihres Arbeitgebers übermitteln. Verantwortliche und Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter:innen nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

Internes A1 Regelwerk

Einschlägige interne Policies, Guidelines und Standards sind im Intranet für alle Mitarbeiter:innen zugänglich und von diesen zu beachten.

Need-To-Know-Prinzip

Mitarbeiter:innen dürfen den Zugriff auf personenbezogene Daten nur nach dem „Need-To-Know-Prinzip" erhalten, d.h. ohne diesen Zugriff wäre die ordnungsgemäße Erledigung der ihnen übertragenen Aufgaben nicht durchführbar. Dies setzt eine präzise Festlegung von Aufgaben, Zuständigkeiten und dafür notwendigen Berechtigungen voraus.

Besondere Kategorien personenbezogener Daten (ehemals „sensible Daten")

Besondere Kategorien personenbezogener Daten sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist grundsätzlich untersagt und muss rechtlich ausdrücklich erlaubt oder vorgeschrieben sein oder die Betroffenen haben ausdrücklich der Verarbeitung zugestimmt. Nach Möglichkeit sind keine besonderen Kategorien personenbezogener Daten zu erheben.

Automatisierte Entscheidungen im Einzelfall

Automatisierte Verarbeitungen personenbezogener Daten dürfen nicht die ausschließliche Grundlage für Entscheidungen bilden, sofern diese Entscheidungen gegenüber Betroffenen rechtliche Wirkungen entfalten. Dies gilt dann nicht, wenn gesetzliche Regelungen eine solche Vorgehensweise erlauben. Betroffene müssen jedoch die Möglichkeit haben (z.B. im A1 Shop, per Anruf, E-Mail), ihren Standpunkt zu dieser Entscheidung darzulegen.

[2] § 6 Datenschutzgesetz - DSG

Werbung

Für die Nutzung personenbezogener Daten für Werbezwecke ist eine Einwilligung der Betroffenen einzuholen, sofern die Nutzung nicht durch gesetzliche Regelungen erlaubt ist. Legen Betroffene einen Widerspruch gegen die Verarbeitung zu Werbezwecken ein, ist eine Nutzung der Daten für diese Zwecke nicht mehr zulässig. A1 gestaltet die Kundenprozesse so, dass der Widerruf einer Einwilligung für Kund:innen nicht schwieriger zu bewerkstelligen ist als ihre Erteilung.

9 Organisation des Datenschutzes

Jeder A1 Vorstand ist für die datenschutzkonforme Verarbeitung personenbezogener Daten in seinen Fachbereichen verantwortlich.

Zur operativen Umsetzung der Datenschutzanforderungen hat deshalb jeder Fachbereich Datenschutz-Bereichskoordinator:innen zu nominieren. Diese sind Ansprechpartner für alle Belange des Datenschutzes und der Datensicherheit im jeweiligen Fachbereich und melden allfällige Schwachstellen und Verstöße an die zuständige Stelle im Unternehmen.

A1 nutzt zahlreiche Applikationen, um die Services und Dienstleistungen automatisiert und qualitätsgesichert zu erbringen. Für jede Applikation sind Applikations-Datenschutzverantwortliche zu benennen, die für die Umsetzung der operativen Datenschutz- und Datensicherheitsanforderungen, z.B. Definition und Implementierung eines Berechtigungskonzeptes, Sorge tragen.

Eigene Organisationseinheiten unterstützen das Management der A1 bei der Einhaltung seiner datenschutzrechtlichen Verpflichtungen und gewährleisten die Informationssicherheit.

Der oder die **Datenschutzbeauftragte** ist bei der Erfüllung der mit dieser Rolle verbundenen Aufgaben nicht weisungsgebunden und darf wegen der Erfüllung dieser Aufgaben nicht abberufen oder benachteiligt werden. Der oder die Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene.

Die Aufgaben des Datenschutzbeauftragten sind insbesondere:

a) die Unterrichtung und Beratung des Vorstandes und der Beschäftigten hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften;

b) die Überwachung der Einhaltung der Datenschutzvorschriften, sowie die Sensibilisierung und Schulung der Mitarbeiter und der diesbezüglichen Überprüfungen;

c) auf Anfrage die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;

d) die Zusammenarbeit mit der Aufsichtsbehörde;

e) die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde und gegebenenfalls Beratung zu allen sonstigen Fragen.

Der oder die Datenschutzbeauftragte ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden.

10 Sanktionen

Die Einhaltung der Datenschutzvorschriften wird von A1 regelmäßig überprüft.

Die missbräuchliche Verarbeitung oder Weitergabe personenbezogener Daten kann für Mitarbeiter:innen disziplinäre, arbeitsrechtliche, aber auch zivil- und strafrechtliche Konsequenzen nach sich ziehen.

11 Publizität

Diese Richtlinie wird im Internet und im Intranet veröffentlicht.

12 Fragen und Hinweise zu dieser Richtlinie

Fragen und Hinweise zu dieser Richtlinie können an den Datenschutzbeauftragten der A1 gerichtet werden. Diesen erreichen Sie unter

datenschutz@a1.at

13 Versionshistorie

Version 1.0		
	Erstellung	Freigabe
Dokument - Version 1.0	Data Privacy	Gesamtvorstand
		25. Mai 2018
Version 1.1		
Dokument - Version 1.1	Data Privacy	Director Legal
gültig ab: Freigabedatum		11. Dezember 2023
Änderungen zu Version 1.0	Neu: Kapitel Datenschutz und Datensicherheit Aktualisierung im Kapitel „Organisation des Datenschutzes Diverse kleinere Anpassungen und Klarstellungen im gesamten Dokument Gendergerechte Sprache im gesamten Dokument	

ANHANG – Begriffserklärungen und Rechtsquellen

Auftragsverarbeiter

Ist eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet (Datenverarbeitung im Auftrag).

Automatisierte Entscheidungen im Einzelfall

Sind Entscheidungen, die für Betroffene rechtliche Folgen nach sich ziehen oder sie wesentlich beeinträchtigen und sich ausschließlich auf eine automatisierte Verarbeitung von Daten stützen, mit denen bestimmte persönliche Aspekte hinsichtlich der Betroffenen bewertet werden, wie die berufliche Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit, Verhalten etc.

Betroffener

Jede natürliche oder juristische Person, die mittels der verarbeiteten Daten identifiziert oder identifizierbar wird.

Dritter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Empfänger

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Inhaltsdaten

Inhalte übertragener Nachrichten.

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche oder juristische Person beziehen**.**

Standortdaten

Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Endeinrichtung von Benutzer:innen eines öffentlichen Kommunikationsdienstes angeben. Standortdaten sind auch Verkehrsdaten.

Verarbeitung von personenbezogenen Daten

Ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder

eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; dies beinhaltet auch die Verarbeitung von personenbezogenen Daten in strukturierten, manuell erstellten Dateien.

Verantwortlicher

Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Verkehrsdaten

Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden, z.B. aktive-/passive Teilnehmernummer, Art des Endgerätes, Zeit und Dauer der Verbindung, Datenmenge.

Rechtsquellen

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) idgF.
- Telekommunikationsgesetz 2021 (TKG 2021) idgF.
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Verkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung - DSGVO)