A1 Richtlinie Datenschutz

Sichere Daten und transparente Regelungen

25. Mai 2018

öffentlich

Version 1.0

Inhalt

Mit der zur besseren Lesbarkeit verwendeten männlichen Form sind immer beide Geschlechter gemeint.

Präambel

Sichere Daten und transparente Regelungen

Für ein Telekommunikationsunternehmen ist es von besonderer Bedeutung, das Vertrauen der Kunden, Geschäftspartner und Mitarbeiter in den sicheren und sensiblen Umgang mit ihren Daten zu rechtfertigen.

Daher gelten für uns drei Handlungsmaximen:

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

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

☐ 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 **(„Zweckbindung")**;

☐ werden nur dem Zweck angemessen verarbeitet sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt **(„Datenminimierung")**;

☐ müssen immer sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; sachlich unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen **(„Richtigkeit")**;

☐ dürfen in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich oder gesetzlich geboten 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")**.

1 Zielsetzung der Richtlinie

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

Kunden, Geschäftspartner und Mitarbeiter vertrauen darauf, dass wir mit ihren Daten sorgfältig umgehen. Dies beinhaltet die Ergreifung von geeigneten technischen und organisatorischen Maßnahmen, um personenbezogene Daten so zu speichern, dass diese für Dritte nicht zugänglich und vor Zerstörung oder Verlust geschützt sind. Es ist jedem Mitarbeiter strikt untersagt, personenbezogene Daten, die ihm im Rahmen seines Dienstverhältnisses anvertraut worden sind, für private Zwecke zu nutzen oder sie Unbefugten zugänglich zu machen.

2 Geltungsbereich

Diese Richtlinie ist für alle Mitarbeiter der A1 Telekom Austria AG verbindlich. Sie gilt für den Umgang mit allen personenbezogenen Daten, insbesondere Daten von Kunden, Geschäftspartnern und Mitarbeitern.

3 Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Betroffene hat seine 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 eines berechtigten Interesses, z.B. der Durchsetzung offener Forderungen. Dies gilt nicht, falls es einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen, insbesondere wenn es sich um ein Kind handelt. Dies ist für jede Verarbeitung zu prüfen. Im Zweifel ist der Datenschutzbeauftragte hierbei zu Rate zu ziehen.

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

Es ist jedem Mitarbeiter strikt untersagt, personenbezogene Daten für private Zwecke zu nutzen oder sie Unbefugten zugänglich zu machen.

4 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 Datenschutz, Informationssicherheit, Telekommunikationsgeheimnis sowie die diesbezüglichen Kontrollrechte vereinbart sind und insbesondere festgehalten ist, dass die personenbezogenen Daten nur nach den Weisungen des Auftraggebers verarbeitet werden dürfen. Wir verwenden 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), so ist die in Abstimmung mit der Rechtsabteilung möglich.

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

5 Übermittlung personenbezogener Daten

Die Weitergabe von personenbezogenen Daten an einen Dritten bedarf einer rechtlichen Grundlage. Diese kann sich auch aus einer gesetzlichen Verpflichtung, der Erfüllung einer vertraglichen Verpflichtung gegenüber dem Betroffenen, oder aus seiner Einwilligung ergeben. Vor der Weitergabe von Daten müssen angemessene Datenschutz- und Informationssicherheitsmaßnahmen gewährleistet sein.

Andere Konzerngesellschaften sind im Sinne des Datenschutzes gesehen wie Dritte zu betrachten.

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

6 Rechte von Betroffenen

Jeder Betroffene hat hinsichtlich seiner personenbezogenen Daten folgende Rechte:

Er kann gegenüber A1 Telekom Austria schriftlich insbesondere **Auskunft** verlangen:

- über die zu seiner Person gespeicherten Daten, inkl. ihrer Herkunft;
- über den Zweck der Verarbeitung oder Nutzung;
- an wen seine Daten übermittelt werden;
- über die Dauer der Speicherung.

Er hat ein Recht auf **Richtigstellung** seiner Daten, falls sie unrichtig oder unvollständig sind.

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

Er hat ein **grundsätzliches Widerspruchsrecht** gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse der verarbeitenden Stelle überwiegt. Das gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

Er hat ein Recht auf **Datenübertragbarkeit**, welches ihn berechtigt ohne Behinderung die Daten, die er einem Verantwortlichen bereitgestellt hat, zu einem anderen Verantwortlichen mitzunehmen.

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

7 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 (z.B. Fangschaltung).

Alle Mitarbeiter 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 des Dienst- oder sonstigen Vertragsverhältnisses fort.

Datengeheimnis[2]

Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter 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 dürfen personenbezogene Daten nur aufgrund einer ausdrücklichen Anordnung ihres Arbeitgebers übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter 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 einzuhalten.

Interne Richtlinien

Einschlägige interne Richtlinien, wie insbesondere die Bestimmungen der internen A1 Information Security Guidelines, sind im Intranet für alle Mitarbeiter zugänglich und sind zu beachten.

Need-To-Know-Prinzip

Mitarbeiter 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 notwendige Berechtigungen voraus.

[1] § 93 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003 idgF.
[2] § 6 Datenschutzgesetz 2018

Datenqualität, Datenminimierung und Zweckbindung

Personenbezogene Daten müssen jederzeit korrekt sein. Unrichtige oder unvollständige Daten müssen gelöscht oder gegebenenfalls berichtigt werden.

Personenbezogene Daten dürfen nur im erforderlichen Umfang erhoben und verarbeitet werden.

Personenbezogene Daten dürfen nur für diejenigen Zwecke verwendet werden, für die sie ursprünglich erhoben wurden bzw. für diejenigen Zwecke, denen der Kunde ursprünglich zugestimmt hat. Sobald personenbezogene Daten für diese(n) Zweck(e) nicht mehr benötigt werden, sind sie zu löschen oder zu anonymisieren, es sei denn, eine Archivierung ist rechtlich erforderlich.

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, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Die Verarbeitung sensibler besonderer Kategorien personenbezogener Daten muss rechtlich ausdrücklich erlaubt oder vorgeschrieben sein oder der Betroffene hat ausdrücklich der Verarbeitung zugestimmt. Nach Möglichkeit sind keine besonderen Kategorien personenbezogener Sensiblen 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, wie z.B. bei der Kreditwürdigkeit. Der Betroffene muss jedoch die Möglichkeit haben (z.B. im A1 Shop, per Anruf, E-Mail), seinen Standpunkt zu dieser Entscheidung darzulegen.

Werbung

Für die Nutzung personenbezogener Daten für Werbezwecke ist eine Einwilligung des Betroffenen einzuholen, sofern die Nutzung nicht durch gesetzliche Regelungen erlaubt ist. Legt der Betroffene einen Widerspruch gegen die Verarbeitung zu Werbezwecken ein, ist eine Nutzung seiner Daten für diese Zwecke nicht mehr zulässig. Wir gestalten unsere Kundenprozesse so, dass der Widerruf einer Einwilligung für den Kunden nicht schwerer zu bewerkstelligen ist als ihre Erteilung.

8 Organisation des Datenschutzes

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

Zur operativen Umsetzung der Datenschutzanforderungen hat deshalb jeder Fachbereich einen Datenschutz-Bereichskoordinator zu nominieren. Dieser ist Ansprechpartner für alle Belange des Datenschutzes und der Informationssicherheit im Fachbereich und meldet allfällige Schwachstellen und Verstöße der Organisationseinheit Data Privacy bzw. der Abteilung Transition Management.

Bei A1 gibt es zahlreiche Applikationen, um die Services und Dienstleistungen automatisiert und qualitätsgesichert erbringen zu können. Für jede Applikation ist ein Applikations-Datenschutz-verantwortlicher zu benennen, der für die Umsetzung der operativen Datenschutz- und Informationssicherheitsanforderungen, z.B. Definition und Implementierung eines Berechtigungskonzeptes, Sorge trägt.

Die Organisationseinheit **Data Privacy** unterstützt das Management der A1 bei der Einhaltung seiner datenschutzrechtlichen Verpflichtungen.

Die Agenden der Informationssicherheit werden bei A1 zentral von der im Fachbereich Network angesiedelten Abteilung **Transition Management** gesteuert und gemeinsam mit allen Security relevanten Organisationseinheiten in Network und anderen Fachbereichen der A1 wahrgenommen.

Die rechtliche Beratung, Vertragsgestaltung, AGB, Straf- und Verwaltungsverfahren sowie Prozessführung sind Aufgaben des Fachbereichs **Legal**.

Der **Datenschutzbeauftragte** ist bei der Erfüllung seiner Aufgaben nicht weisungsgebunden, und darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der 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 Datenschutzbeauftragte ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden

9 Sanktionen

Die Einhaltung der Datenschutzrichtlinien und der geltenden Datenschutzgesetze wird regelmäßig überprüft.

Die missbräuchliche Erhebung, Verarbeitung oder Nutzung personenbezogener Daten kann disziplinäre, arbeitsrechtliche, aber auch -, zivil- und strafrechtliche Konsequenzen nach sich ziehen.

10 Publizität

Diese Richtlinie wird im Internet und im Intranet veröffentlicht.

11 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@a1telekom.at

12 Historie

Datum	Maßnahme
25. Mai 2018	In Kraft Setzung durch den Vorstand

ANHANG – Begriffserklärungen und Rechtsquellen

Automatisierte Entscheidungen im Einzelfall

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

Betroffener

Jede natürliche Person, die mittels ihrer bei der A1 Telekom verwendeten Daten, identifiziert oder identifizierbar wird.

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).

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 und Telefonate

Personenbezogene Daten

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

Besondere Kategorie personenbezogener Daten (als Sonderform personenbezogener Daten)

Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Standortdaten

Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung angeben. Standortdaten sind auch Verkehrsdaten.

Umgang mit personenbezogenen Daten

Ist jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie die Erhebung, Aufzeichnung, Organisation, Speicherung, Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination, Verknüpfung, Sperrung, Löschung oder Vernichtung; dies beinhaltet auch die Verarbeitung von personenbezogenen Daten in strukturierten, manuell erstellten Dateien.

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.

Gesetze, auf denen diese Richtlinie basiert bzw. worauf sie Bezug nimmt

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) idgF.

- Telekommunikationsgesetz 2003 (TKG 2003) 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:
  http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE