Technische und organisatorische Maßnahmen des Datenschutzes
Anlage zum Auftragsverarbeitungsvertrag (AVV) (Szenario 3)

Deutsche Telekom AG

Version 3.0
Stand 01.12.2021
Status final

öffentlich

Erleben, was verbindet.

Impressum

Herausgeber

Deutsche Telekom AG
Group Privacy

Dateiname	Dokumentennummer	Dokumentenbezeichnung
AVV Anhang TOM S3 v03 fin.docx	v 3.0	Anlage TOM (Szenario 3) zum AVV-Vertrag

Version	Stand	Status
3.0	01.12.2021	final

Autor

Group Privacy
Bonn, Dezember 2021

Kurzinfo

Dieses Dokument ist nur gültig als Anlage eines Vertrags zur Datenverarbeitung im Auftrag

Inhaltsverzeichnis

1. Einleitung

Die in diesem Dokument definierten technischen und organisatorischen Maßnahmen (TOM) sind eine Ergänzung zu den im AVV-Rahmenvertrag vereinbarten Regelungen (zur Ausgestaltung der in Artikel 32 definierten Anforderungen der DSGVO). Für die Verarbeitung im Auftrag gelten die Vorgaben des AVV-Rahmenvertrags vollumfänglich. Abhängig vom vorliegenden Szenario gelten die in diesen Anhang definierten Anforderungen zusätzlich. Grundsätzlich wird in den Anhängen zum AVV-Rahmenvertrag zwischen den folgenden Szenarien unterschieden:

- Szenario 1: Der Auftragsverarbeiter nutzt allein oder zusätzlich die eigene (bzw. die eines Unterauftragsverarbeiters/Dritten) IT-Infrastruktur (Server/Client, Anwendung) oder die eigenen Endgeräte. Oder: Der Auftragsverarbeiter oder ein von ihm Beauftragter speichern in der eigenen IT-Infrastruktur oder in eigenen Endgeräten personenbezogene Daten des Verantwortlichen.
- Szenario 2: Der Auftragsverarbeiter nutzt die IT-Infrastruktur (Server/Client, Anwendung) des Verantwortlichen und greift mittels eigener (bzw. die eines Unterauftragsverarbeiters) End-Geräte auf diese zu. Es erfolgt keine Datenspeicherung beim Auftragsverarbeiter oder einem Dritten.
- Szenario 3: Der Auftragsverarbeiter nutzt ausschließlich die IT-Infrastruktur (Server/Client, Anwendung) und End-Geräte des Verantwortlichen Auftraggebers.

Dieser Anhang zum Rahmen-AVV oder Gesamt-AVV bezieht sich auf das Szenario 3, mit den folgenden Voraussetzungen:

- Der Auftragsverarbeiter nutzt ausschließlich die IT-Infrastruktur (Server/Client, Anwendung) und End-Geräte des Verantwortlichen.

- Es erfolgt keine Datenspeicherung beim Auftragsverarbeiter oder einem Dritten.

- Der Auftragsverarbeiter erfüllt zudem die folgenden als verpflichtend markierten Anforderungen der Deutschen Telekom zur Umsetzung der technischen und organisatorischen Maßnahmen.

1.1 Anwendungshinweise

Die in Kapitel 2 definierten Maßnahmen konkretisieren die Anforderungen des Art. 32 DSGVO und seiner Schutzziele. Die Ausgestaltung der Ziele ist sowohl von Art, Menge und Form der zu verarbeitenden Daten als auch den jeweiligen örtlichen Gegebenheiten abhängig. Je nach Art der Auftragsverarbeitung können sich weitere Anforderungen für den Auftragsverarbeiter ergeben. Diese können sektorspezifische (z.B. Gesundheitswesen, Bankensektor), länderspezifische (z.B. länderspezifische Gesetze) oder zusätzliche spezifische Anforderungen des Telekom Konzerns sein.
Die nachfolgenden Anforderungen gliedern zu jedem Gewährleistungsziel die korrespondierenden Maßnahmen.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben (i. d. R. im Rahmen der Bestellung abzuschließen).

1.2 Begriffsklärung

In den Anforderungsdefinitionen zu den technischen und organisatorischen Maßnahmen wird zwischen normalem und hohem Schutzbedarf unterschieden. Ein hoher Schutzbedarf liegt vor, wenn:

- die Verarbeitung personenbezogener Daten unter die besonderen Kategorien nach DSGVO Artikel 9, Absatz 1 fällt,
- und/oder die Form der Verarbeitung die Kriterien erfüllen, die eine Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erfordern, bspw. mindestens bei Vorliegen einer der folgenden Fallgestaltungen:
    - systematische Überwachung / Scoring / Profiling,
    - Datentransfer in Länder außerhalb der EU / des EWR,
    - Verkehrsdaten der Telekommunikation / Nutzungsdaten der Telemedien,
    - Lokalisierungsdaten,
    - zielgerichtete Leistungs- und Verhaltenskontrolle von Beschäftigten,
    - Kontodaten von Personen, Personalausweis / Reisepass,
    - Vertragsdaten, wie Kundennummer, Geburtsdatum,
    - sensible Daten von Beschäftigten wie Führungszeugnis, Altersversorgungsdaten, Personalnummer, Zeiterfassung,
    - umfangreiche Datensätze z. B. bei privater Anschrift/Telefonnummer.

Sind personenbezogene Daten uneinheitlich in ihrem Schutzbedarf, das heißt, einzelne Bestandteile gehören unterschiedlichen Schutzklassen an, so ist die höchste Schutzklasse maßgebend. Nach ihr richten sich die zu ergreifenden Schutzmaßnahmen.

2. Technische und organisatorische Maßnahmen

Gewährleistungsziel 1 – Verfügbarkeit

Das Gewährleistungsziel "Verfügbarkeit" bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können.

Req 1.1 Personalkonzept zur Gewährleistung der Schutzziele

Der Auftragsverarbeiter hat ein Personalkonzept umgesetzt, das den Datenschutz durch die folgenden Maßnahmen unterstützt:

- Es wird nur fachkundiges Personal eingesetzt, das alle notwendigen Schulungen und Verpflichtungen auf Vertraulichkeit und das Fernmeldegeheimnis nachweisen kann.
- Es gibt für jede Verarbeitung personenbezogener Daten einen verantwortlichen Ansprechpartner. Eine Vertreterregelung existiert.
- Beschäftigte und Auftragsverarbeiter geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrags oder der Vereinbarung die in ihrem Besitz befindlichen Werte an die Organisation (Verantwortlicher/Auftragsverarbeiter) zurück, die ihnen zur Erfüllung der Aufgabe überlassen wurden. Zu diesen gehören Zutrittsmittel, Rechner, Speichermedien und mobile Endgeräte.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Gewährleistungsziel 2 – Integrität

Das Gewährleistungsziel "Integrität" bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. "Integrität" bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben.

Req 2.1 Berechtigungskonzept

Der Auftragsverarbeiter nutzt aktuelle Berechtigungskonzepte die verbindlich vorgeben, wer wann auf welche Systeme, Datenbanken oder Netze Zugriff hat. Das Berechtigungskonzept muss dabei folgenden Eigenschaften genügen:

- Es gibt definierte Berechtigungen in Form von Rollen auf Basis der geschäftlichen, sicherheitsrelevanten und datenschutzrechtlichen Anforderungen.
- Die Rollen sind dokumentiert und aktuell.
- Rollen werden Nutzern oder Maschinen eindeutig zugeordnet.
- Benutzer haben ausschließlich Zugang zu den Netzwerken, Systemen und Daten zu deren Nutzung sie ausdrücklich befugt sind.
- Ein formaler Prozess für die Registrierung und Deregistrierung ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.
- Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
- Die Zuteilung und der Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird fortlaufend kontrolliert.

- Die Zuteilung von Zugangsrechten unterliegt der Kontrolle, mit dem Ziel eine funktionsübergreifende Rechtezuweisung zu verhindern.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Req 2.2 Identitätsmanagement

Die Zuteilung einer Berechtigung für den Zugriff auf personenbezogene Daten erfolgt erst nach einer eindeutigen Identifizierung des Benutzers. Benutzer können eindeutig von einem System identifiziert werden. Dies wird dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto genutzt wird. Sogenannte Gruppenkonten, d.h. die Nutzung eines Benutzerkontos für mehrere Personen werden nicht verwendet.
Eine Ausnahme dieser Anforderung sind die sogenannte Maschinenkonten. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer einzelnen Person zugewiesen werden. Solche Benutzerkonten werden individuell pro System oder pro Anwendung vergeben. Hierbei wird sichergestellt, dass eine missbräuchliche Nutzung solcher Benutzerkonten nicht möglich ist.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Gewährleistungsziel 3 – Vertraulichkeit

Das Gewährleistungsziel "Vertraulichkeit" bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der jeweiligen betroffenen Person haben.

In dem vorliegenden Szenario werden die Maßnahmen zur Sicherstellung der Vertraulichkeit durch die verantwortliche Stelle sichergestellt.

Gewährleistungsziel 4 – Nichtverkettung

Das Gewährleistungsziel "Nichtverkettung" bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden. Je größer und aussagekräftiger Datenbestände sind, umso größer können die Begehrlichkeiten sein, die Daten über die ursprüngliche Rechtsgrundlage hinaus zu nutzen.

In dem vorliegenden Szenario werden die Maßnahmen zur Sicherstellung der Nichtverkettung durch die verantwortliche Stelle sichergestellt.

Gewährleistungsziel 5 – Transparenz

Das Gewährleistungsziel "Transparenz" bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen

erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Req 5.1 Dokumentation der Datenverarbeitung

Der Auftragsverarbeiter dokumentiert die Verarbeitung personenbezogener Daten wie folgt:

- Der Verarbeitungsprozess ist so dokumentiert, das vollständig nachvollziehbar ist, wie die Verarbeitung personenbezogener Daten umgesetzt ist. Dies bezieht sich auf den gesamten Verarbeitungszyklus von der Übernahme/Erzeugung personenbezogener Daten bis hin zur deren Weitergabe/Löschung.
- Es erfolgt eine Dokumentation im Fall von Störungen, Problembearbeitungen, sowie Änderungen an Verarbeitungstätigkeiten oder den technischen und organisatorischen Maßnahmen
- Es ist zudem dokumentiert wer zu welchem Zeitpunkt Zugriff auf die Daten hat.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Req 5.2 Dokumentation und Speicherung von Verträgen, Vereinbarungen, Weisungen

Der Auftragsverarbeiter legt alle Verträge, Vereinbarungen oder Weisungen sicher ab, d.h. diese sind jederzeit für die Vertragspartner oder Aufsichtsbehörden verfügbar.

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Gewährleistungsziel 6 – Intervenierbarkeit

Das Gewährleistungsziel "Intervenierbarkeit" bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

Req 6.1 Implementierung von Maßnahmen zur Umsetzung von Betroffenenrechten im Systemdesign (Privacy by Design)

Der Auftragsverarbeiter beachtet beim Systemdesign die Umsetzung der Betroffenenrechte und Anforderungen des Datenschutzes. Die folgenden Maßnahmen müssen beim Systemdesign (Prozesse und Software) umgesetzt werden:

- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken.
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können
- Deaktivierungsmöglichkeit einzelner Funktionen ohne Mitleidenschaft für das Gesamtsystem.

- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- Entfernen nicht notweniger Datenfelder und Optionen, Reduktion der Ausgabe nach Suchanfragen in Datenbanken, Minimierung von Export- und Druckfunktionen

Kann eine Maßnahme nicht oder nur teilweise umgesetzt werden, sind eine Begründung und die Angabe alternativer Maßnahmen ***in der dem Verwendungszweck entsprechenden TOMs der Einzel-AVV anzugeben*** *(i. d. R. im Rahmen der Bestellung abzuschließen).*

Gewährleistungsziel 7 – Datenminimierung

Das Gewährleistungsziel "Datenminimierung" erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Die Umsetzung dieses Minimierungsgebots hat einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms.

In dem vorliegenden Szenario werden die Maßnahmen zur Datenminimierung durch die verantwortliche Stelle sichergestellt.