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

Deutsche Telekom AG

Version 2.0
Stand 01.06.2020
Status final

öffentlich

Erleben, was verbindet.

Impressum

Herausgeber

Deutsche Telekom AG
Group Privacy

Dateiname	Dokumentennummer	Dokumentenbezeichnung
AVV Anhang TOM S3 v02 final.docx	v 2.0	Anlage TOM (Szenario 3) zum AVV-Vertrag

Version	Stand	Status
2.0	01.06.2020	final

Autor

Group Privacy
Bonn, Juni 2020

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. Bei der Interpretation der Requirements sind die Vorgaben der ISO/IEC 27001:2017-06, der ISO/IEC 27002:2017-06, der ISO/IEC 27701:2019(E) und der ISO/IEC 29151:2017 (E) maßgeblich, dies gilt auch für Sachverhalte, die nicht von den Requirements abgedeckt sind. 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.

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

01 Regelungen und Maßnahmen zum Gebrauch von Informationen und Werten, welche die Verarbeitung personenbezogener Daten ermöglichen

Die Organisation hat Regelungen definiert und umgesetzt, welche Informationen und Werte (Daten, technische Einrichtungen, Versorgungseinrichtungen, etc.) die zur Verarbeitung personenbezogener Daten genutzt werden vor unbefugtem Zugriff, unbefugter Modifikation, Verlust oder Zerstörung oder falscher und gesetzwidriger Verarbeitung schützen. Diese Regelungen beziehen sich auf den gesamten Lebenszyklus von Information und Werten.

Bezug/Referenzen	
DSGVO	Artikel 32, Abs. 1 a-c und Artikel 6 Abs. 4 (Vertraulichkeit, Verfügbarkeit, Integrität, Pseudonymisierung, Verschlüsselung)
ISO/IEC 27001:2017-06	Tabelle A1: A.8.1.3
ISO/IEC 29151:2017 (E)	8.1.4

02 Rückgabe von Werten

Beschäftigte und Auftragsverarbeiter geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrags oder der Vereinbarung die in ihrem Besitz befindlichen Werte an die Organisation zurück, die ihnen zur Erfüllung der Aufgabe überlassen wurden. Zu diesen gehören Zutrittsmittel, Rechner, Speichermedien und mobile Endgeräte.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 b und Artikel 28, Abs. 3 g (Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.8.1.4
ISO/IEC 29151:2017 (E)	8.1.5