Technische und organisatorische Maßnahmen des Datenschutzes
Anlage zum Auftragsverarbeitungsvertrag (AVV) (Szenario 1)

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 S1 v02 final.docx	v 2.0	Anlage TOM (Szenario 1) 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 nur 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 1, mit den folgenden Voraussetzungen:

- Der Auftragsverarbeiter nutzt allein oder zusätzlich die eigene (bzw. die eines weiteren Auftragsverarbeiters) IT-Infrastruktur (Server/Client, Anwendung) oder die eigenen End-Geräte.

- Der Auftragsverarbeiter oder ein Dritter verarbeiten im eigenen Verantwortungsbereich personenbezogene Daten des Verantwortlichen.

- 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 Richtlinien zum Informations- und Datenschutz

In der Organisation sind durch die Leitung oder Geschäftsführung verbindliche Richtlinien zur Umsetzung des Datenschutzes und der Informationssicherheit festgelegt. Diese Richtlinien sind schriftlich fixiert, frei zugänglich, allen internen und externen Beschäftigten bekannt gemacht und werden angewendet.
Die Vorgaben zu Datenschutz und Informationssicherheit werden regelmäßig auf Wirksamkeit, Aktualität und Regelkonformität hin geprüft.

Bezug/Referenzen	
DSGVO	Artikel 32
ISO/IEC 27001:2017-06	Tabelle A1: A.5.1.1, A.5.1.2
ISO/IEC 29151:2017 (E)	5.1.2, 5.1.3

02 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

03 Richtlinien und Maßnahmen zur Nutzung von Mobilgeräten und Telearbeitsplätzen

Gemessen an den identifizierten Risiken der Nutzung von Mobilgeräten (Laptops, externe Speichermedien, Mobiltelefone) sind geeignete Richtlinien und Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität personenbezogener Daten in der Organisation umgesetzt. Ziel dieser Regelungen ist,

- den Zugriff auf personenbezogene Daten zu minimieren,
- deren Speicherung und Übertragung zu verschlüsseln,
- und die Nutzung externer Speichermedien auf das Notwendige zu reduzieren.

Bezug/Referenzen	
DSGVO	Artikel 32, Abs. 1 b (Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.6.2.1, A.6.2.2
ISO/IEC 29151:2017 (E)	6.2.2, 6.2.3

04 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

05 Handhabung von Datenträgern

Verfahren für die Handhabung von Datenträgern sind entsprechend dem identifizierten Schutzbedarf umgesetzt.
Bei Speicherung von personenbezogenen Daten auf mobilen Datenträgern sind diese in der Regel zu verschlüsseln, jedenfalls dann, wenn personenbezogene Daten mit hohem Schutzbedarf gespeichert werden.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 a-b (Verschlüsselung, Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.8.3.1
ISO/IEC 29151:2017 (E)	8.3.2

06 Transport von Datenträgern

Der Transport von Datenträgern muss sich an dem Schutzbedarf der zu übermittelnden personenbezogenen Daten orientieren. Soweit personenbezogene Daten nicht verschlüsselt sind, müssen angemessene Schutzmaßnahmen ergriffen werden.
Bei hohem Schutzbedarf bestehen besondere Anforderungen an die Zuverlässigkeit des Transportes, die Verpflichtung zur Verschlüsselung von Daten, Dokumentations-, Protokoll- und Nachweispflichten.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 a-b (Vertraulichkeit, Integrität, Verschlüsselung)
ISO/IEC 27001:2017-06	Tabelle A1: A.8.3.3
ISO/IEC 29151:2017 (E)	8.3.4

07 Zugangskontrolle

Eine Zugangssteuerungsrichtlinie wird auf Grundlage der datenschutzrechtlichen und sicherheitsrelevanten Anforderungen in der Organisation erstellt und umgesetzt.
Diese Richtlinie regelt den Zugang zu personenbezogenen Daten in Abhängigkeit von deren Schutzbedarf auf den zur Aufgabenerfüllung minimalen Umfang (need to know). Dazu gehört insbesondere der Zugriff auf IT-Systeme, Netzwerke und Datenbanken mit personenbezogenen Daten.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs.1 (Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.9.1.1, A.9.4.1
ISO/IEC 29151:2017 (E)	9.1.2, 9.4.2

08 Zugang zu Netzwerken, Systemen und Diensten

Der Zugang zu Netzwerken, Systemen (z.B. Server, Endgeräte, Datenbanken) und deren Diensten ist eingeschränkt. Der Zugang wird nur den Nutzern gewährt, die zur Nutzung berechtigt sind (Berechtigungskonzept). Die Zugangssteuerung wird durch die folgenden technischen und organisatorischen Maßnahmen umgesetzt:

- Es erfolgt eine personengebundene Benutzerregistrierung und Deregistrierung (keine anonymen Benutzer wie z.B. Consultant #1 oder Extern#2).
- In der Organisation ist die Benutzerregistrierung durch verbindliche Vorgaben oder Prozesse geregelt und dokumentiert.
- Es gibt in der Organisation Regelungen zur Vergabe von Nutzerzugängen (z.B. need to know, privilegierte Zugänge, unzulässige Rollenkombinationen).
- Es gibt Vorgaben zur Erteilung, Nutzung, Entzug und Dokumentation von Zugangsberechtigungen und den Gebrauch von Authentisierungsinformationen.
- Regelungen zum dauerhaften Schutz der Vertraulichkeit und Integrität von Authentisierungsinformationen sind umgesetzt.
- Die Einhaltung der Regelungen zur Benutzerregistrierung und Berechtigungsvergabe wird regelmäßig überprüft (z.B. Überprüfung "alter" Berechtigungen, Test auf Doppelregistrierungen, Missbrauchserkennung).
- Diese Schutzmaßnahmen schließen auch Telearbeitsplätze mit ein.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 b, d (Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit)
ISO/IEC 27001:2017-06	Tabelle A1: A.9.1.2, A.9.2., A.9.2.2, A.9.2.3, A.9.2.4,A.9.2.5, A.9.2.6
ISO/IEC 29151:2017 (E)	9.1.3, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7

09 Datenschutzgerechtes Anmeldeverfahren

Der Zugang zu Systemen und Anwendungen wird durch ein sicheres Anmeldverfahren umgesetzt.
Das Anmeldeverfahren berücksichtigt den Schutzbedarf der personenbezogenen Daten. Bei hohem Schutzbedarf sind Anmeldeverfahren anzuwenden, die auf Besitz und Wissen (Zwei-Faktor-Authentisierung) basieren. Bei geringerem Schutzbedarf ist eine Authentisierung durch Benutzername und Passwort ausreichend.
Werden Systeme zur Verwaltung und Vergabe von Kennwörtern genutzt, so stellen diese starke Kennwörter sicher. Erfolgt der Zugang durch Hilfsprogramme, automatisiert oder durch Routinen in der Softwareentwicklung, dann wird der Gebrauch auf das notwendige Mindestmaß reduziert und die Anwendung regelmäßig überwacht.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 b, d (Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit)

ISO/IEC 27001:2017-06	Tabelle A1: A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5
ISO/IEC 29151:2017 (E)	9.4.3, 9.4.4, 9.4.5, 9.4.6

10 Regelungen zum Gebrauch kryptografischer Maßnahmen

In der Organisation ist der Gebrauch kryptografischer Maßnahmen zum Schutz personenbezogener Daten durch eine Richtlinie entwickelt und umgesetzt. Diese Richtlinie regelt und gewährleistet:

- den angewandten Stand der Technik kryptografischer Verfahren,
- den erforderlichen Schutzbedarf der personenbezogenen Daten auf Basis einer Risikoeinschätzung,
- die Verwaltung und Anwendung kryptografischer Schlüssel,
- die Schutzziele kryptografischer Schlüssel über deren gesamten Lebenszyklus (die Erzeugung, Speicherung, Anwendung und Vernichtung).

Bezug/Referenzen

DSGVO	Artikel 32 Abs. 1 a, b (Pseudonymisierung, Verschlüsselung, Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.10.1.1, A.10.1.2
ISO/IEC 29151:2017 (E)	10.1.2, 10.1.3

11 Zutrittssteuerung

In der Organisation sind Bereiche in Abhängigkeit des Schutzbedarfs definiert, die notwendigen Sicherheitsperimeter definiert und umgesetzt. Der Schutzbedarf richtet sich nach den in den Bereichen (einschließlich Telearbeitsplätze) befindlichen personenbezogenen Daten oder informationsverarbeitenden Systemen.
Es sind geeignete Zutrittssteuerungsvorgaben definiert und angewendet, die sicherstellen, dass nur berechtigte Personen Zutritt zu den definierten Bereichen erhalten.

Bezug/Referenzen

DSGVO	Artikel 32 Abs. 1 b, d und Abs. 2 (Vertraulichkeit, Integrität, Verfügbarkeit)
ISO/IEC 27001:2017-06	Tabelle A1: A.11.1.1, A.11.1.2, A.11.1.3
ISO/IEC 29151:2017 (E)	11.1.2, 11.1.3, 11.1.4

12 Schutz vor in- und externen Bedrohungen

In der Organisation sind Maßnahmen zum Schutz vor internen und externen Bedrohungen konzipiert und umgesetzt. Dies umfasst den Schutz:

- vor Naturkatastrophen, Angriffen oder Unfällen,
- vor Störungen etwa durch Stromausfälle oder anderen Versorgungseinrichtungen,
- der Verkabelung vor Unterbrechung, Störung oder Beschädigung.

Bezug/Referenzen

DSGVO	Artikel 32 Abs. 1 b-d (Verfügbarkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.11.1.4, A.11.2.2, A.11.2.3
ISO/IEC 29151:2017 (E)	11.1.5, 11.2.3, 11.2.4

13 Trennung von und in Entwicklungs-, Test- und Betriebsumgebungen

Entwicklungs-, Test- und Betriebsumgebungen sollen zumindest logisch getrennt sein. Es sollen geeignete Zugangskontrollen implementiert werden, um sicherzustellen, dass der Zugang auf ordnungsgemäß autorisierte Personen beschränkt ist. Innerhalb dieser Umgebungen sind die personenbezogenen Daten dieser Auftragsverarbeitung von anderen zu trennen. Diese Trennung ist entweder physikalisch oder logisch umzusetzen.
Wenn Test- oder Entwicklungsnetzwerke oder -geräte den Zugriff auf das betriebliche Netzwerk erfordern, sollen starke Zugriffskontrollen implementiert werden.
Soweit nicht durch Gesetz oder Einwilligung des Betroffenen erlaubt, dürfen personenbezogene Daten in Test- und Entwicklungsumgebungen nicht ohne vorherige Anonymisierung verarbeitet werden.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs.1 a, b, d (Integrität, Vertraulichkeit, Pseudonymisierung)
ISO/IEC 27001:2017-06	Tabelle A1: A.12.1.4
ISO/IEC 29151:2017 (E)	12.1.5

14 Maßnahmen gegen Schadsoftware

Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt und informationsverarbeitende Systeme sind gehärtet. Zum Schutz der Systeme ist geeignete Software (z.B. Virenscanner, IDS) installiert und aktuell. Bei einer Systemhärtung sind mindestens die folgenden Punkte zu beachten:

- aktueller Patchstand,
- alle nicht benötigten Softwareelemente sind zu deinstallieren,
- alle nicht benötigten Dienste sind zu deinstallieren/deaktivieren,
- alle benötigten Dienste sind nach Möglichkeit auf die Interfaces zu binden, wo sie benötigt werden,
- nicht benötigte voreingestellte Dienstkonten sind zu löschen und voreingestellte Passwörter zu ändern.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 b (Vertraulichkeit, Integrität, Verfügbarkeit)
ISO/IEC 27001:2017-06	Tabelle A1: A.12.2.1
ISO/IEC 29151:2017 (E)	12.2.2

15 Sicherung von Informationen und Daten

In der Organisation sind Regelungen definiert und angewendet, die eine geeignete Backup-Strategie sicherstellen. Diese berücksichtigt insbesondere Anforderungen an die Verfügbarkeit des Systems, die regelmäßige Überprüfung der Wiederherstellbarkeit sowie gesetzliche Vorgaben an Speicherung oder Löschung.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs.1 b- c (Verfügbarkeit)
ISO/IEC 27001:2017-06	Tabelle A1: A.12.3.1
ISO/IEC 29151:2017 (E)	12.3.2

16 Protokollierung

Zugriffe von Benutzern und Systemadministratoren auf personenbezogene Daten müssen unter Berücksichtigung des Grundsatzes der Datenminimierung und des Schutzbedarfs
protokolliert und regelmäßig überprüft werden. Der Zugriff sowie die Art des Zugriffs (z.B. Lesen, Ändern, Löschen) ist zu protokollieren.
Relevante Ereignisse, Ausnahmen, Störungen und Informationssicherheitsvorfälle sind ebenfalls zu protokollieren und regelmäßig zu überprüfen.
Die Protokolle werden so abgelegt, dass der Zugriff durch die protokollierten Systemadministratoren oder Benutzer auf die Protokolle nicht möglich ist.

Bezug/Referenzen

DSGVO	Artikel 32, Abs. 1 b, d (Vertraulichkeit, Integrität)
ISO/IEC 27001:2017-06	Tabelle A1: A.12.4.1, A.1.4.2, A.12.4.3
ISO/IEC 29151:2017 (E)	12.4.2, 12.4.3, 12.4.4
ISO/IEC 27701:2019 (E)	Tabelle B1: B.8.2.6

17 Kommunikationssicherheit

In der Organisation gibt es Richtlinien, Sicherheitsverfahren und Steuerungsmaßnahmen, um die Übertragung von Informationen für alle Arten von Kommunikationseinrichtungen (einschließlich Telearbeitsplätzen) zu schützen. Bei elektronischer Nachrichtenübermittlung wurden die folgenden Anforderungen umgesetzt:

- Netzwerke werden verwaltet und gesteuert,
- Sicherheits- und Qualitätsanforderungen wurden definiert und vereinbart,
- Netzwerke wurden separiert (Nutzergruppen, Dienste),
- Maßnahmen zum Schutz personenbezogener Daten wurden definiert und umgesetzt (Verschlüsselung, Pseudo- und Anonymisierung).

Bezug/Referenzen

DSGVO	Artikel 32 Abs. 1 a,b,d (Vertraulichkeit, Integrität, Verfügbarkeit, Pseudonymisierung, Verschlüsselung)
ISO/IEC 27001:2017-06	Tabelle A1: A.13.1.1, A.13.1.2, A.13.1.3, A.13.2.1, A.13.2.3
ISO/IEC 29151:2017 (E)	13.1.2, 13.1.3, 13.1.4, 13.2.2, 13.2.4

18 Maßnahmen zur Aufrechterhaltung der Informations- und Datensicherheit

In der Organisation sind Datenschutz und -sicherheit so in das Business Continuity Management integriert, dass Prozesse, Verfahren und Maßnahmen auch in widrigen Situationen eine vertragsgemäße Auftragsverarbeitung sicherstellen. Die Organisation überprüft diese regelmäßig auf Wirksamkeit und stellt die Verfügbarkeit, z.B. durch Redundanzen sicher.

Bezug/Referenzen	
DSGVO	Artikel 32 Abs. 1 a-d (Verfügbarkeit, Belastbarkeit)
ISO/IEC 27001:2017-06	Tabelle A1: A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
ISO/IEC 29151:2017 (E)	17.1.2, 17.1.3, 17.1.4, 17.2.2