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

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 S1 v03 fin.docx	v 3.0	Anlage TOM (Szenario 1) 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 in den EU-Standardvertragsklauseln vereinbarten Regelungen (zur Ausgestaltung der in Artikel 32 definierten Anforderungen der DSGVO). Für die Verarbeitung im Auftrag gelten die Vorgaben der EU-Standardvertragsklauseln vollumfänglich. Abhängig vom vorliegenden Szenario gelten die in diesem Anhang definierten Anforderungen zusätzlich. Grundsätzlich wird in den Anhängen zu den EU-Standardvertragsklauseln 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. 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 Physischer Schutz vor äußeren Einflüssen

Beim Auftragsverarbeiter sind Maßnahmen zum Schutz vor internen und externen Bedrohungen konzipiert und umgesetzt. Diese dienen dem Schutz:

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

Die Maßnahmen zum physischen Schutz müssen regelmäßig auf Wirksamkeit hin getestet wurden. Zudem ist das Schutzkonzept bei Änderungen der Datenverarbeitung anzupassen. Entsprechende Prozesse müssen beim Auftragsverarbeiter umgesetzt sein.

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 1.2 Schutz der IT-Systeme und Netze vor äußeren Einflüssen

Der Auftragsverarbeiter hat Regelungen definiert und umgesetzt, welche IT-Systeme, Netze und Komponenten (technische Einrichtungen, Versorgungseinrichtungen, etc.) die zur Verarbeitung personenbezogener Daten genutzt werden vor unbefugtem Zugriff, unbefugter Modifikation, Verlust oder Zerstörung oder falscher und gesetzwidriger Nutzung schützen. Diese Regelungen beziehen sich auf den gesamten Lebenszyklus.
Zudem wurden Datenschutz und -sicherheit so in das Business Continuity Management integriert, dass Prozesse, Verfahren und Maßnahmen auch in widrigen Situationen eine vertragsgemäße Auftragsverarbeitung sicherstellen. Der Auftragsverarbeiter überprüft diese regelmäßig auf Wirksamkeit und stellt die Verfügbarkeit, z.B. durch Redundanzen sicher.

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 1.3 Systemhärtung

Informationen 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 umgesetzt:

- Der Patchstand ist aktuell.
- Bei der Installation eines Systems werden oftmals Software-Komponenten installiert oder auch einzelne Teile einer Software aktiviert, die für den Betrieb und die Funktion des Systems nicht notwendig sind. Solche Komponenten wurden entweder bei der Installation nicht mit installiert oder wurden nach der Installation entfernt. Des Weiteren wurde keine Software auf den Systemen installiert, die nicht für den Betrieb, die Wartung oder Funktion des Systems notwendig ist.
- Neben Funktionen der Software sind nach der Systeminstallation auch keine Hardware-Funktionen aktiviert, die nicht für den Einsatz des Systems benötigt werden. Solche Funktionen, wie beispielsweise nicht benötigte Schnittstellen, wurden dauerhaft deaktiviert, so dass sie auch nach einem Neustart deaktiviert bleiben.
- Sämtliche auf einem System und den Schnittstellen nicht erforderliche Dienste wurden vollständig deaktiviert und bleiben auch nach einem Neustart des Systems weiterhin deaktiviert.
- Die Erreichbarkeit eines Dienstes über die erforderlichen Schnittstellen wurde zudem auf legitime Kommunikationspartner eingeschränkt,
- nicht benötigte voreingestellte Dienstkonten gelöscht und voreingestellte Passwörter geändert.
- Es ist üblich, dass auf Systemen Authentisierungsmerkmale wie Passwörter und kryptographische Schlüssel durch Hersteller, Entwickler oder Lieferanten vorkonfiguriert werden. Solche Authentisierungsmerkmale wurden in eigene, Dritten nicht bekannte Merkmale geändert.
- Wird das System auf einer Cloud-Plattform betrieben, wurde verhindert, dass das System (bzw. der komplette Mandant/Tenant mit all seinen Diensten und Daten) versehentlich oder durch Unbefugte vollständig gelöscht werden kann.

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 1.4 Backup-Konzept

Der Auftragsverarbeiter hat 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.
Ziel dieser Maßnahme ist es, ein konsistentes Abbild der Wirkdaten in Notfall sicherzustellen. Hier können, abhängig von den Rahmenbedingungen, verschiedene Strategien zur Anwendung kommen. Neben einer klassischen Backuplösung ist auch der Betrieb von Spiegelsystemen in einem anderen Sicherheitsbereich, oder eine Kombination aus beiden Strategien möglich.

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 1.5 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).*

Req 1.6 Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit

Der Auftragsverarbeiter hat ein Notfallkonzept zur Wiederherstellung der Datenverarbeitung implementiert. Ziel dieses Konzepts ist die Wiederherstellung der Verfügbarkeit nach einer Störung der Verarbeitung. Das Notfallkonzept genügt dabei den folgenden Anforderungen/Kriterien:

- Es gibt Vorgaben, in denen nach einer Störung die Zeit bis zur Wiederherstellung der geregelten Datenverarbeitung festgelegt ist.
- Die Bereitstellung von Ressourcen zur Wiederherstellung ist erfolgt.
- Die Zuordnung von Verantwortlichkeiten ist erfolgt.
- Die Definition von geprüften Maßnahmen zur Abwehr der Störung und Wiederherstellung des Regelbetriebs ist erfolgt.
- Informations- und Eskalationsketten existieren
- Definition der Interaktion mit korrespondierenden Prozessen und Regelungen (Backupkonzept, Personalkonzept, ...) ist erfolgt.

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 Definition, Anwendung, und Kontrolle des Sollverhaltens von Prozessen

Der Auftragsverarbeiter hat durch seine Leitung oder Geschäftsführung verbindliche Prozesse zur Umsetzung des Datenschutzes und der Informationssicherheit festgelegt. Diese sind schriftlich fixiert, frei zugänglich, allen internen und externen Beschäftigten bekannt gemacht und werden angewendet. Ziel der Vorgaben ist es, die Verarbeitung von personenbezogenen Daten so umzusetzen, dass das definierte

Sollverhalten der Prozesse jederzeit gewährleistet ist. Die Vorgaben werden regelmäßig auf Wirksamkeit, Aktualität und Regelkonformität hin geprüft.

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 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 2.3 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).*

Req 2.4 Kryptokonzept

Der Auftragsverarbeiter hat den Gebrauch kryptografischer Maßnahmen zum Schutz personenbezogener Daten durch eine Richtlinie definiert und umgesetzt. Diese Richtlinie regelt und gewährleistet:

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

Ziel eines solchen Kryptokonzepts ist es:

- die Integrität schutzbedürftiger Daten sicherzustellen
- Prozesse des Identitätsmanagements abzusichern
- Authorisierungsprozesse zu unterstützen
- Die Vertraulichkeit und Integrität schutzbedürftiger Daten sicherzustellen

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 2.5 Prozesse zur Aufrechterhaltung der Aktualität von Daten

Der Auftragsverarbeiter hat Prozesse definiert, umgesetzt und kommuniziert, die die Aktualität der personenbezogenen Daten sicherstellen und den folgenden Anforderungen genügen:

- Anfragen zu Berichtigungen, Änderungen und Löschungen durch den Betroffenen erfolgen zeitnah und über alle gespeicherten Datensätze.
- Änderungen oder Löschungen personenbezogener Daten erfolgen automatisiert oder prozessgesteuert über alle gespeicherten Datensätze.
- Erfolgte Änderungen an Daten mit Personenbezug sind über Zeitstempel voneinander unterscheidbar.
- Speicherdauer und Löschfristen sind gemäß den gesetzlichen oder vertraglichen Vorgaben festgelegt.

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.

Req 3.1 Festlegung und Kontrolle der Nutzung zugelassener Ressourcen und Kommunikationskanäle

Der Auftragsverarbeiter stellt durch die folgenden Maßnahmen sicher, dass die für die Verarbeitung personenbezogener Daten genutzten Ressourcen und Kommunikationskanäle festgelegt sind und deren Nutzung kontrolliert wird:

- Bereiche sind in Abhängigkeit des Schutzbedarfs definiert, die notwendigen Sicherheitsperimeter vorgegeben und umgesetzt. Die Schutzbedarfseinstufung richtet sich nach den in den Bereichen (einschließlich mobiler Arbeitsplätze) 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.
- Eine Zugangssteuerungsrichtlinie ist 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.
- Verfahren für die Handhabung von Datenträgern sind entsprechend dem identifizierten Schutzbedarf umgesetzt.
- Bei Speicherung von personenbezogenen Daten auf mobilen Datenträgern werden diese wirksam (vgl. 2.4) verschlüsselt.
- Es gibt Vorgaben zum Transport von Datenträgern, die sich an dem Schutzbedarf personenbezogenen Daten orientieren. Soweit personenbezogene Daten nicht verschlüsselt sind, werden angemessene alternative Schutzmaßnahmen ergriffen. Bei hohem Schutzbedarf bestehen besondere Anforderungen an die Zuverlässigkeit des Transportes, die Verpflichtung zur Verschlüsselung von Daten, Dokumentations-, Protokoll- und Nachweispflichten.
- Es existieren Richtlinien, Sicherheitsverfahren und Steuerungsmaßnahmen, um die Übertragung von Informationen für alle Arten von Kommunikationseinrichtungen (einschließlich mobiler Arbeitsplätze) zu schützen. Bei der Übertragung personenbezogener Daten über öffentliche Netzwerke, werden diese immer verschlüsselt.
- 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 es, den Zugriff auf personenbezogene Daten zu minimieren, deren Speicherung und Übertragung zu verschlüsseln und die Nutzung externer Speichermedien auf das Notwendige zu reduzieren.

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 3.2 Sichere Authentifizierungsverfahren

Der Zugang zu Systemen und Anwendungen wird durch ein sicheres Authentisierungsverfahren umgesetzt. Das Authentisierungsverfahren berücksichtigt den Schutzbedarf der personenbezogenen Daten, auf die nach erfolgreicher Authentisierung zugegriffen werden kann. Bei hohem Schutzbedarf sind Anmeldeverfahren anzuwenden, die auf Besitz und Wissen (Zwei-Faktor-Authentisierung) basieren. Von hohem Schutzbedarf ist auszugehen, wenn der Zugriff auf Daten ermöglicht wird, die unter Art. 9 Abs. 1 der DSGVO fallen. Bei geringerem Schutzbedarf ist eine Authentisierung durch Benutzername und Passwort ausreichend. Grundsätzlich genügt das gewählte Authentisierungsverfahren den folgenden Kriterien:

- Alle Benutzerkonten des Systems werden vor einer Nutzung durch Unberechtigte geschützt. Hierfür wird das Benutzerkonto mit einem Authentisierungsmerkmal abgesichert, welches eine eindeutige Authentifizierung des zugreifenden Benutzers ermöglicht. Authentisierungsmerkmale sind z.B.: Passwörter, Passphrases, PINs, (Faktor Wissen) /Kryptographische Schlüssel, Token, Smartcards, OTP (Besitz)/oder Biometrische Merkmale wie etwa Fingerabdrücke oder die Hand-Geometrie (Inhärenz)
- Die Vorgaben für die Erzeugung/Erstellung von Passwörtern (Länge, Komplexität, Wiederverwendung, etc.) richten sich mindestens nach dem aktuellen Stand der Technik
- Beim Einsatz von Passwörtern als Authentisierungsmerkmal ist ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden
- Das System bietet Funktionen, die es dem Benutzer ermöglicht das Passwort jederzeit zu ändern.
- Passwörter werden unter Verwendung einer für diesen Zweck geeigneten, nach aktuellem Stand der Technik als sicher eingestuften, kryptografischen Einwegfunktion gespeichert (bekannt als "Password-Hashing" Verfahren)
- Werden Systeme zur Verwaltung und Vergabe von Kennwörtern genutzt, so stellen diese die Verwendung starker Kennwörter sicher. Erfolgt der Zugang durch Hilfsprogramme, automatisiert oder durch Routinen in der Softwareentwicklung, dann wird der Gebrauch dieser auf das notwendige Mindestmaß reduziert und die Anwendung regelmäßig überwacht.
- Benutzer welche über erweiterte Berechtigungen innerhalb eines Systems verfügen, wie etwa einen Zugriff auf personenbezogene Daten mit einem hohen Schutzbedarf, Konfigurationseinstellungen oder Administrationszugänge bekommen, um ein angemessenes Schutzniveau zu erreichen, mindestens zwei voneinander unabhängige Authentisierungs-merkmale. Die verwendeten Authentisierungsmerkmale müssen aus unterschiedlichen Faktoren (Wissen, Besitz, Inhärenz) bestehen. Dieser Ansatz wird allgemein als MFA (Multi-Faktor-Authentisierung) bezeichnet. Eine spezifische Form der MFA ist die 2FA (2-Faktor-Authentisierung), die exakt zwei Authentisierungsmerkmale kombiniert. Eine Kombination von Authentisierungsmerkmalen desselben Faktors (z.B. zwei unterschiedliche Passwörter) ist nicht zulässig.

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 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.

Req 4.1 Definition und Festlegung des Verarbeitungszwecks

Der Auftragsverarbeiter stellt durch geeignete Maßnahmen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten nur im Rahmen des vertraglich vereinbarten Zwecks verarbeitet werden. Zu diese Maßnahmen zählen:

- interne Dokumentation und Kommunikation des Verwendungszwecks in allen Datenverarbeitungsverfahren
- geregelte Zweckänderungsverfahren

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 4.2 Maßnahmen zur Sicherstellung der Zweckbindung

Der Auftragsverarbeiter stellt sicher, dass personenbezogene Daten ausschließlich zu dem vertraglich vereinbarten Zwecken verarbeitet werden und nur zur Verarbeitung befugte Personen/Instanzen Zugriff auf die Daten haben. Neben den definierten Anforderungen zu den Gewährleistungszielen Verfügbarkeit, Integrität und Vertraulichkeit wurden folgende Maßnahmen getroffen, um eine Verkettung von Datensätzen mit unterschiedlicher Zweckbindung zu vermeiden:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten auf das zur Verarbeitung zwingend notwendige Maß
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung von Umgebungen mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und mittels sicherer Authentifizierungsverfahrens
- Entwicklungs-, Test- und Betriebsumgebungen müssen zumindest logisch getrennt sein. Es wurden geeignete Zugangskontrollen implementiert, um sicherzustellen, dass der Zugang auf ordnungsgemäß autorisierte Personen beschränkt ist. Innerhalb dieser Umgebungen wurden die personenbezogenen Daten dieser Auftragsverarbeitung von anderen getrennt. Diese Trennung wurde entweder physikalisch oder logisch umgesetzt.
- Wenn Test- oder Entwicklungsnetzwerke oder -geräte den Zugriff auf das betriebliche Netzwerk erfordern, wurden starke Zugriffskontrollen implementiert.
- Die Verarbeitung personenbezogener Daten in Test- und Entwicklungsumgebungen ist ausgeschlossen. Ausnahmen sind durch eine separate schriftliche Weisung des Auftraggebers zu definieren.

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 4.3 Definition, Einführung und Anwendung von Anonymisierungsverfahren

Der Auftragsverarbeiter organisiert die Datenverarbeitung so, dass personenbezogenen Daten nur unter Berücksichtigung der Zweckbindung verarbeitet werden. Ist eine Zweckbindung nicht gegeben, werden nicht benötigte Daten gelöscht. Sollte eine Löschung nicht möglich sein, werden die entsprechenden Datensätze anonymisiert. Dazu dient der Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials und die Verarbeitung pseudonymer bzw. anonymisierter Daten sowie die Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren. Zu beachten ist, dass das Mittel der Pseudonymisierung nur in wenigen Fällen rechtlich zulässig 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 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 Verfahrensverzeichnis

Der folgende Auszug aus Art. 30 der DSGVO wurde beim Auftragsverarbeiter vollständig umgesetzt:
"Der Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Das genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
Die in den genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es

erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 DSGVO"

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 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 5.3 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).*

Req 5.4 Protokollierung der Datenverarbeitung

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

Req 5.5 Sicherstellung der Auskunftspflichten

Der Auftragsverarbeiter hat einen Prozess implementiert, der das Auskunftsrecht eines Betroffenen gemäß der Vorgaben Art. 15 DSGVO unterstützt. Dieser Prozess wird regelmäßig auf seine Wirksamkeit hin überprüft.

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 Prozessimplementation zur Umsetzung der Betroffenenrechte

Der Auftragsverarbeiter hat Maßnahmen der Wahrung von Betroffenenrechten implementiert. Grundsätzlich sind die im Folgenden genannten Maßnahmen geeignet:

- Sofern nicht bereits durch den Verantwortlichen umgesetzt, hat der Auftragsverarbeiter einen Prozess zur Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten implementiert.
- Verantwortlicher und Auftragsverarbeiter definieren gemeinsam ein Merkmal, mit dem Betroffene eindeutig über Organisationsgrenzen hinweg identifiziert werden kann.
- Der Auftragsverarbeiter hat Systeme, Software und Prozesse so implementiert, dass Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten möglich sind.
- Der Auftragnehmer hat die operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten implementiert.
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen.

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 6.2 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.

Req 7.1 Operative Maßnahmen zur Datenminimierung

Der Auftragsverarbeiter ergreift operative Maßnahmen, mit dem Ziel die Verarbeitung personenbezogener Daten zweckgebunden auf ein Minimum zu beschränken. Folgende Maßnahmen sind umzusetzen:

- Beschränkung der erfassten Attribute der betroffenen Personen auf das erforderliche Minimum
- Bei Weitergabe personenbezogener Daten werden nur solche Attribute weitergegeben, die für den Verarbeitungszweck des nachfolgenden Prozessschritts unbedingt notwendig sind.

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 7.2 Technische Maßnahmen zur Datenminimierung

Der Auftragsverarbeiter ergreift technische Maßnahmen, mit dem Ziel die Verarbeitung personenbezogener Daten zweckgebunden auf ein Minimum zu beschränken. Folgende Maßnahmen sind geeignet:

- Beschränkung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Anwendung von Pseudonymisierungs- und Anonymisierungsverfahren
- Beschränkung von Möglichkeiten der Kenntnisnahme vorhandener Daten (Anzeigeoptionen, Suchfelder, ...) auf das erforderliche Minimum

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 7.3 Definition, Implementation und Kontrolle eines Löschkonzeptes

Der Auftragsverarbeiter erstellt für jede Verarbeitung personenbezogener Daten ein Löschkonzept, das Folgendes beinhaltet:

- Nennung der zu löschenden Datenfelder
- Definition von Löschfristen
- Kontrolle und Nachweis der Löschung
- Verantwortliche Personen

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).*