AVV ANHANG 1

—

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

STAND: MAI 2022

—

Das gegenständliche Dokument ergänzt die zwischen AG und AN abgeschlossene Auftragsverarbeitungsvereinbarung (AVV) gemäß Art 28 DSGVO (EU-Datenschutzgrundverordnung).

Die technischen und organisatorischen Maßnahmen werden von Anexia entsprechend Art 32 DSGVO umgesetzt. Sie werden von Anexia laufend nach Machbarkeit und Stand der Technik – nicht zuletzt auch im Sinne der aktiven ISO 27001 Zertifizierung – verbessert und auf ein höheres Sicherheits- und Schutzniveau gebracht.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen

- ✓ Alarmanlage
- ✓ Automatisches Zugangskontrollsystem
- ✓ Biometrische Zutrittskontrolle Rechenzentrum
- ✓ Chipkarten / Transpondersysteme
- ✓ Manuelles Schließsystem
- ✓ Türen mit Knauf Außenseite
- ✓ Klingelanlage mit Kamera
- ✓ Videoüberwachung der Eingänge

Organisatorische Maßnahmen

- ✓ Schlüsselregelung / Liste
- ✓ Empfang / Rezeption / Pförtner
- ✓ Besucherbuch / Protokoll der Besucher
- ✓ Mitarbeiter- / Besucherausweise
- ✓ Besucher in Begleitung durch Mitarbeiter
- ✓ Sorgfalt bei Auswahl des Wachpersonals
- ✓ Sorgfalt bei Auswahl Reinigungsdienste

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.11.1 Sicherheitsbereiche, A11.2 Geräte und Betriebsmittel

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen

- ✓ Login mit Benutzername + Starkes Passwort
- ✓ Anti-Viren-Software Server
- ✓ Anti-Virus-Software Clients
- ✓ Anti-Virus-Software mobile Geräte
- ✓ Firewall
- ✓ IDS im Einsatz (Intrusion Detection Systeme)
- ✓ IPS im Einsatz (Intrusion Prevention Systeme)
- ✓ Einsatz VPN bei Remote-Zugriffen
- ✓ Verschlüsselung von Datenträgern
- ✓ Verschlüsselung Smartphones
- ✓ Automatische Desktopsperre
- ✓ Verschlüsselung von Festplatten bei Notebooks / Tablets / Smartphones
- ✓ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen

Organisatorische Maßnahmen

- ✓ Verwalten von Benutzerberechtigungen
- ✓ Zentrales Erstellen von Benutzerprofilen
- ✓ Passwortgeschützte Useraccounts
- ✓ Anwendung von Sicherheitsmaßnahmen für Telearbeit nach Stand der Technik
- ✓ Eingeschränkte Nutzung von administrativen Useraccounts

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.6.2 Mobilgeräte und Telearbeit, A.9.1 Geschäftsanforderungen an die Zugangssteuerung, A.9.2 Benutzerzugangsverwaltung, A.9.3 Benutzerverantwortlichkeiten, A.9.4 Zugangssteuerung für Systeme und Anwendungen, A.10.1 Kryptographische Maßnahmen, A.12.1 Betriebsabläufe und -verantwortlichkeiten, A.12.2 Schutz vor Schadsoftware, A.12.4 Protokollierung und Überwachung, A.12.5 Steuerung von Software im Betrieb, A.12.7 Audit von Informationssystemen, A.13.1 Netzwerksicherheitsmanagement, A.13.2 Informationsübertragung

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- ✓ Aktenshredder mind. empfohlene Sicherheitsstufe P-4 (DIN 66399)
- ✓ Externe Aktenvernichtung mind. Sicherheitsstufe P-4 (DIN 66399)
- ✓ Physische Löschung von Datenträgern Sicherheitsstufe H-4 (DIN66399)
- ✓ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- ✓ Zugriffe auf Systeme mittels SSH
- ✓ TLS Verschlüsselung

Organisatorische Maßnahmen

- ✓ Einsatz Berechtigungskonzepte
- ✓ Minimale Anzahl an Administratoren
- ✓ Verwaltung Benutzerrechte durch Administratoren
- ✓ Anwendung kryptografischer Verfahren nach aktuellem Stand der Technik

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.8.2 Informationsklassifizierung, A.8.3 Handhabung von Datenträgern, A.9.2 Benutzerzugangsverwaltung, A.10.1 Kryptographische Maßnahmen, A.12.4 Protokollierung und Überwachung

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen

- ✓ Trennung von Produktiv- und Testumgebung
- ✓ Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- ✓ Mandantenfähigkeit relevanter Anwendungen
- ✓ VLAN-Segmentierung von Netzwerken
- ✓ Kundensysteme logisch getrennt
- ✓ Staging von Entwicklungs-, Test und Produktivumgebung

Organisatorische Maßnahmen

- ✓ Festlegung von Datenbankrechten
- ✓ Definierte Anforderungen für Entwicklungsumgebungen
- ✓ Definierte Anforderungen für die Durchführung von Tests in der Softwareentwicklung

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.9.2 Benutzerzugangsverwaltung, A.12.1 Betriebsabläufe und Verantwortlichkeiten, A.13.1 Netzwerksicherheitsmanagement, A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen, A.14.3 Testdaten

2. Integrität

2.1. Weitergabekontrolle und Eingabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder bzw. Eingabe während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen

- ✓ Einsatz von VPN
- ✓ Protokollierung der Zugriffe und Abrufe
- ✓ Bereitstellung über verschlüsselte Verbindungen wie sftp, https – Secure Cloudstores
- ✓ Technische Protokollierung von Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

- ✓ Umsetzung des Need-to-know Prinzips

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.9.2 Benutzerzugangsverwaltung, A.10.1 Kryptographische Maßnahmen, A.12.4 Protokollierung und Überwachung, A.13.2 Informationsübertragung

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (USV, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.).

Technische Maßnahmen

- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöscher Serverraum
- ✓ Serverraumüberwachung Temperatur und Feuchtigkeit
- ✓ Serverraum klimatisiert
- ✓ USV-Anlage und Notstrom-Dieselaggregate RZ
- ✓ Schutzsteckdosenleisten Serverraum
- ✓ RAID System / Festplattenspiegelung
- ✓ Videoüberwachung Serverraum
- ✓ Einsatz von Schutzprogrammen gegen Schadsoftware

Organisatorische Maßnahmen

- ✓ Bestehende Notfallvorsorgeplanung
- ✓ Regelmäßige Tests der Dieselaggregate RZ

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.11.1 Sicherheitsbereiche, A.12.1 Betriebsabläufe und -verantwortlichkeiten, A.12.2 Schutz vor Schadsoftware, A.12.3 Datensicherung, A.12.4 Protokollierung und Überwachung, A.17.1 Aufrechterhalten der Informationssicherheit, A.17.2 Redundanzen

3.2. Wiederherstellbarkeit

Maßnahmen, die dazu befähigen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Technische Maßnahmen

- ✓ Backup-Monitoring und -Reporting
- ✓ Wiederherstellbarkeit aus Automatisierungs-Tools

Organisatorische Maßnahmen

- ✓ Recovery-Konzept
- ✓ Kontrolle des Sicherungsvorgangs

- ✓ Backup-Konzept nach Kritikalität und Kundenvorgaben
- ✓ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.12.3 Datensicherung, A.12.4 Protokollierung und Überwachung, A.17.1 Aufrechterhalten der Informationssicherheit, A.17.2 Redundanzen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutzmanagement

Technische Maßnahmen

- ✓ Zentrale Dokumentation aller Regelungen zum Datenschutz mit technischer Zugriffsmöglichkeit für Mitarbeiter
- ✓ Jährliche Überprüfung der Angemessenheit der TOM

Organisatorische Maßnahmen

- ✓ Datenschutzmanagementsystem implementiert
- ✓ Informationssicherheitsmanagement implementiert

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.5.1 Vorgaben der Leitung für Informationssicherheit, A.6.1 Interne Organisation, 18.1.4 Privatsphäre und Schutz von personenbezogener Information, 18.2 Überprüfungen der Informationssicherheit

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.

Technische Maßnahmen

- ✓ Einsatz von Firewall und regelmäßige Aktualisierung
- ✓ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ✓ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ✓ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung
- ✓ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung

Organisatorische Maßnahmen

- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheits- und Datenschutzvorfällen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.12.2 Schutz vor Schadsoftware, A.12.6 Handhabung technischer Schwachstellen, A.13.1 Netzwerksicherheitsmanagement, A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen, A.18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

4.3. Datenschutzfreundliche Voreinstellungen

„Privacy by design" / „Privacy by default" gem. Art 25 Abs 2 DSGVO.

Technische Maßnahmen

- ✓ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware

Organisatorische Maßnahmen

- ✓ Dokumentierte Anforderungen an „Privacy by design / default" sind vorhanden
- ✓ Anforderungen für sichere Softwareentwicklungen sind definiert

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.14.1 Sicherheitsanforderungen an Informationssysteme, A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen, A.18.2 Überprüfungen der Informationssicherheit

4.4. Auftragskontrolle (Outsourcing, Subauftragnehmer und Auftragsverarbeitung)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen

- ✓ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support
- ✓ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln 1, 2

Organisatorische Maßnahmen

- ✓ Lieferantenbewertungen werden risikobasiert durchgeführt
- ✓ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- ✓ Auswahl des Auftragnehmers auf Basis definierter Kriterien
- ✓ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- ✓ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe
- ✓ Regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus

Die Maßnahmen referenzieren auf folgende Kontrollen (Annex A) aus der IEC/ISO 27001:2013: A.13.2 Informationsübertragung, A.15.1 Informationssicherheit in Lieferantenbeziehungen, A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten, A.18.1.4 Privatsphäre und Schutz von personenbezogener Information

5. Zertifizierungen

Sowohl das **Qualitätsmanagementsystem nach ISO 9001** als auch das **Informationssicherheitsmanagementsystem nach ISO 27001** wesentlicher Teile von **Anexia inkl. DATASIX Rechenzentrumsbetrieb** sind durch die unabhängige TÜV NORD CERT GmbH **zertifiziert**.

Maßnahme	Nach ISO 27001 & ISO 9001 zertifiziert
Zutrittskontrolle	✓
Zugangskontrolle	✓
Zugriffskontrolle	✓
Weitergabekontrolle	✓
Eingabekontrolle	✓
Auftragskontrolle	✓
Verfügbarkeitskontrolle	✓
Trennungskontrolle	✓
Innerbetriebliche Organisation	✓