AVV ANHANG 1

—

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

STAND: November 2023

—

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 (betrifft ANX04)
- ✓ 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

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
- ✓ Firewalls mit Intrusion Detection/Intrusion Prevention Systemen (IDS/IPS)
- ✓ Einsatz von 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 nach dem Need-to-Know-Prinzip
- ✓ Zentrales Erstellen und Verwalten von Benutzerprofilen
- ✓ User- und Passwortrichtlinien
- ✓ Anwendung von Sicherheitsmaßnahmen für Telearbeit nach Stand der Technik
- ✓ Eingeschränkte Nutzung von administrativen Useraccounts
- ✓ Zutrittsordnungen für Office Standorte und Rechenzentren

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

- ✓ Zentrale Benutzer- und Berechtigungsverwaltung
- ✓ Verschlüsselung von data-at-rest und data-in-transit
- ✓ Logging und Monitoring

Organisatorische Maßnahmen

- ✓ Einsatz von Berechtigungskonzepten
- ✓ Minimale Anzahl an Administratoren
- ✓ Verwaltung von Benutzerrechte durch Administratoren
- ✓ Richtlinie für kryptografische Verfahren

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

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
- ✓ Richtlinie für kryptografische Verfahren

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
- ✓ Hochverfügbarkeitssysteme bei kritischen Systemen

Organisatorische Maßnahmen

- ✓ Bestehende Notfallvorsorgeplanung
- ✓ Regelmäßige Wartung und Tests von Klimaanlagen, Löschsystemen, Batterien und Dieselgeneratoren
- ✓ Desaster Recovery Pläne
- ✓ Desaster Recovery Tests

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
- ✓ Backup-Konzept nach Kritikalität und Kundenvorgaben

Organisatorische Maßnahmen

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

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

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.

Technische Maßnahmen

- ✓ Zentraler Meldeweg für Sicherheitsverletzungen und Datenpannen
- ✓ Weitreichendes Logging und Monitoring für forensische Untersuchungen

Organisatorische Maßnahmen

- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheits- und Datenschutzvorfällen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
- ✓ Definierte Rollen und Verantwortlichkeiten in der Organisation
- ✓ Schulung und Sensibilisierung für Mitarbeiter

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

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
- ✓ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe
- ✓ Regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Zertifizierungen

Sowohl das **Qualitätsmanagementsystem nach ISO 9001** als auch das **Informationssicherheitsmanagementsystem nach ISO 27001** wesentlicher Teile von **Anexia sowie des DATASIX Rechenzentrumsbetriebs** sind durch die unabhängige TÜV NORD CERT GmbH **zertifiziert**. Zudem ist das **Datenschutzmanagementsystem nach ISO 27701** wesentlicher Teile von **Anexia sowie des DATASIX Rechenzentrumsbetriebs** durch die unabhängige CIS - Certification & Information Security Services GmbH zertifiziert.