AVV ANHANG 1

—

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

STAND: SEPTEMBER 2020

—

Das gegenständliche Dokument ergänzt das Kapitel 11 der zwischen AG und AN abgeschlossenen 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 Zugangssperren
- ✓ Chipkarten / Transpondersysteme
- ✓ Manuelles Schließsystem
- ✓ Türen mit Knauf Außenseite
- ✓ Klingelanlage mit Kamera
- ✓ Videoüberwachung der Eingänge
- ✓ Biometrische Zutrittskontrolle Rechenzentrum

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
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Arbeitsanweisung Zutrittssteuerung

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
- ✓ Intrusion Detection Systeme
- ✓ Einsatz VPN bei Remote-Zugriffen
- ✓ Verschlüsselung von Datenträgern
- ✓ Verschlüsselung Smartphones
- ✓ Automatische Desktopsperre
- ✓ Verschlüsselung von Notebooks / Tablet
- ✓ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen

Organisatorische Maßnahmen

- ✓ Verwalten von Benutzerberechtigungen
- ✓ Erstellen von Benutzerprofilen
- ✓ Zentrale Passwortvergabe
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung IT-Benutzerordnung
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Arbeitsanweisung Zugangssteuerung
- ✓ Mobile Device Policy

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)
- ✓ Externer Aktenvernichtung mind. Sicherheitsstufe P-6 (DIN 66399)
- ✓ Physische Löschung von Datenträgern
- ✓ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- ✓ Zugriffe SSH Verschlüsselt
- ✓ zertifizierte SSL Verschlüsselung

Organisatorische Maßnahmen

- ✓ Einsatz Berechtigungskonzepte
- ✓ Minimale Anzahl an Administratoren
- ✓ Verwaltung Benutzerrechte durch Administratoren
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Kommunikationssicherheit
- ✓ Arbeitsanweisung Umgang mit Informationen und Werten

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
- ✓ Kundensysteme logisch getrennt
- ✓ Staging von Entwicklungs-, Test und Produktivumgebung

Organisatorische Maßnahmen

- ✓ Steuerung über Berechtigungskonzept
- ✓ Festlegung von Datenbankrechten
- ✓ Richtlinie Informationssicherheit
- ✓ Richtlinie Datenschutz
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Arbeitsanweisung Sicherheit in der Softwareentwicklung

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen

- ✓ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System (verschlüsselt)
- ✓ auf Wunsch des Kunden werden Logfiles pseudonymisiert

Organisatorische Maßnahmen

- ✓ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren
- ✓ Richtlinie Informationssicherheit
- ✓ Richtlinie Datenschutz
- ✓ Separate, explizite Arbeitsanweisung Kryptographie (dzt. in Ausarbeitung)

2. Integrität

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder 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
- ✓ Nutzung von Signaturverfahren (fallabhängig)

Organisatorische Maßnahmen

- ✓ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- ✓ Weitergabe in anonymisierter oder pseudonymisierter Form
- ✓ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
- ✓ Persönliche Übergabe mit Protokoll
- ✓ Richtlinie Informationssicherheit
- ✓ Richtlinie Datenschutz

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen

- ✓ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ✓ Manuelle oder automatisierte Kontrolle der Protokolle (nach strikten internen Vorgaben)

Organisatorische Maßnahmen

- ✓ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- ✓ Klare Zuständigkeiten für Löschungen
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung IT-Benutzerordnung

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige 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 Notrom-Dieselaggregate RZ
- ✓ Schutzsteckdosenleisten Serverraum
- ✓ RAID System / Festplattenspiegelung
- ✓ Videoüberwachung Serverraum
- ✓ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

Organisatorische Maßnahmen

- ✓ Backup-Konzept
- ✓ Keine sanitären Anschlüsse im Serverraum
- ✓ Existenz eines Notfallplans
- ✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ✓ Getrennte Partitionen für Betriebssysteme und Daten, wo notwendig
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Regelmäßige Tests der Dieselaggregate RZ

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

- ✓ Recovery-Konzept
- ✓ Kontrolle des Sicherungsvorgangs
- ✓ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ✓ Existenz eines Notfallplans
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Betriebssicherheit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutzmanagement

Technische Maßnahmen

- ✓ Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- ✓ Sicherheitszertifizierung nach ISO 27001
- ✓ Eine Überprüfung der Wirksamkeit der TOM wird mind. jährlich durchgeführt und TOMs aktualisiert
- ✓ Datenschutzprüfpunkte durchgängig in Tool-gestütztem Risk Assessment implementiert

Organisatorische Maßnahmen

- ✓ Interner Datenschutzbeauftragter bestellt: Group Data Protection Officer, DPO
- ✓ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- ✓ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
- ✓ Interner Informationssicherheits-Beauftragter bestellt: Group Information Security Officer, ISO
- ✓ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- ✓ Prozess betr. Informationspflichten nach Art. 13 und 14 DSGVO etabliert
- ✓ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- ✓ Datenschutzbetrachtung im Rahmen des Corporate Risk Managements etabliert
- ✓ ISO 27001 Zertifizierung wesentlicher Unternehmensteile inkl. RZ-Betrieb und jährliche Überwachungsaudits

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

- ✓ Dokumentierter Prozess zur Erkennung und
- ✓ Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ✓ Einbindung von DPO und ISO in Sicherheitsvorfälle und Datenpannen
- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
- ✓ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
- ✓ Richtlinie Informationssicherheit
- ✓ Richtlinie Datenschutz
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Arbeitsanweisung IT-Benutzerordnung

4.3. Datenschutzfreundliche Voreinstellungen

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

Technische Maßnahmen

- ✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- ✓ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware

Organisatorische Maßnahmen

- ✓ Richtline Datenschutz (inkludiert Prinzipien „Privacy by design / default")
- ✓ OWASP Secure Mobile Development Security Checks werden durchgeführt
- ✓ Perimeteranalyse bei Webapplikationen

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

- ✓ Arbeitsanweisung Lieferantenmanagement und Lieferantenbewertung
- ✓ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- ✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- ✓ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- ✓ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe
- ✓ Schriftliche Weisungen an den Auftragnehmer
- ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- ✓ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ✓ Regelung zum Einsatz weiterer Subunternehmer
- ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ✓ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Organisation und Datenschutz bei Anexia

Die Anexia Unternehmensgruppe hat sich in ihrer **strategischen Leitlinie Qualitäts-, Risiko- und Compliance-Politik** unter anderem zum Ziel gesetzt, ihren Kunden die zu liefernden Produkte und Services auf **höchstmöglichem Informationssicherheitsniveau rechtskonform** zur Verfügung zu stellen. Diese Leitlinie bildet den Rahmen für eine **transparente, nachhaltige, prozessbasierte und risikoorientierte Steuerung** der Unternehmensgruppe im Rahmen eines **Integrierten Management Systems (IMS)**. Anexia hat in diesem Zusammenhang eine ausgeprägte **Sicherheits-Querschnittsorganisation** etabliert, um einen umfassenden Schutz ihrer eigenen Unternehmensinformationen- und Daten sowie den Schutz der Daten ihrer Kunden und Auftraggeber zu gewährleisten. Dabei sind die Funktionen **Information Security Officer (ISO)**, **Data Protection Officer (DPO)**, **Quality Officer (QO), Risk Officer (RO)** sowie **Legal Compliance Officer (LCO)** mit gruppenweiter Verantwortung und direktem Weisungsrecht in diesen Wirkungsbereichen innerhalb der **direkt dem CEO zugeordneten Stabsabteilung „Quality, Risk & Compliance“** eingerichtet und ein umfassendes Regelwerk aus **internen Richtlinien und Regelungen** („**Anexia Corporate Binding Rules**“ u. a. zu Informationssicherheit und Datenschutz) etabliert, das für alle Mitarbeiter verbindlich einzuhalten ist und einen sicheren und datenschutzkonformen Umgang mit Informationen und Daten festlegt. Die **Mitarbeiter** werden laufend **auf dem Gebiet des Datenschutzes informiert und geschult**. Darüberhinausgehend sind alle Mitarbeiter dienstvertraglich zum **Datengeheimnis und zur Geheimhaltung verpflichtet**. **Externe**, die im Rahmen ihrer Tätigkeit für Anexia in Berührung mit personenbezogenen Daten kommen könnten, werden vor Beginn ihrer Tätigkeit zur Verschwiegenheit und Geheimhaltung sowie zur Einhaltung von Datenschutz und Datengeheimnis mittels einem sogenannten **NDA (Non-Disclosure-Agreement) verpflichtet**. Alle verbundenen Unternehmen der Anexia Unternehmensgruppe innerhalb der EU bzw. des EWR haben eine gemeinsame **Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung** als verbindliches schriftliches Rechtsinstrument gemäß Art 28 DSGVO abgeschlossen, um einen einheitlich hohen Datenschutz- und Datensicherheitsstandard über die gesamte Gruppe hinweg zu gewährleisten und die Rechte und Pflichten bei jeglichen Auftragsverarbeitungen klar zu regeln. Jegliche mit weiterer Auftragsverarbeitung betraute Subunternehmen werden erst nach Genehmigung des Verantwortlichen und nach Abschluss einer Auftragsverarbeitungsvereinbarung (AVV) nach Art 28 DSGVO eingesetzt, mit welcher ihnen alle datenschutzrechtlichen Pflichten, denen Anexia selbst unterliegt, vollinhaltlich überbunden werden. All diese organisatorischen Maßnahmen flankieren die jeweils aktuellen, **hohen technischen Sicherheitsstandards** von Anexia und beide Dimensionen werden **periodisch** im Zuge **interner Audits** sowie jährlich im Rahmen der **ISO 9001 und ISO 27001 Überwachungs- bzw. Re-Zertifizierungsaudits** von unabhängigen, externen, **DAkkS-akkreditierten Zertifizierungsstellen** auf ihre Angemessenheit und Wirksamkeit überprüft und bestätigt.

6. 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	DSGVO-konform umgesetzt	Kommentare
Zutrittskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Zugangskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Zugriffskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Weitergabekontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Eingabekontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Auftragskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Verfügbarkeitskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Trennungskontrolle	✓	ISO 27001 & ISO 9001 zertifiziert
Innerbetriebliche Organisation	✓	ISO 27001 & ISO 9001 zertifiziert