anexia

IT SERVICES & SOFTWARE DEVELOPMENT

AVV-ART-28-DSGVO | ANHANG 1

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

VERSION 2 | STAND: MAI 2019

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	Organisatorische Maßnahmen
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Biometrische Zugangssperren	☒ Besucherbuch / Protokoll der Besucher
☒ Chipkarten / Transpondersysteme	☒ Mitarbeiter- / Besucherausweise
☒ Manuelles Schließsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Türen mit Knauf Außenseite	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Klingelanlage mit Kamera	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Videoüberwachung der Eingänge	☒ Richtlinie Informationssicherheit
☒ Biometrische Zutrittskontrolle Rechenzentrum	☒ Arbeitsanweisung Betriebssicherheit
	☒ Arbeitsanweisung Zutrittssteuerung

1.2. Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Starkes Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Viren-Software Server	☒ Erstellen von Benutzerprofilen
☒ Anti-Virus-Software Clients	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software mobile Geräte	☒ Richtlinie Informationssicherheit
☒ Firewall	☒ Arbeitsanweisung IT-Benutzerordnung
☒ Intrusion Detection Systeme	☒ Arbeitsanweisung Betriebssicherheit
☒ Einsatz VPN bei Remote-Zugriffen	☒ Arbeitsanweisung Zugangssteuerung
☒ Verschlüsselung von Datenträgern	☒ Mobile Device Policy
☒ Verschlüsselung Smartphones	
☒ Automatische Desktopsperre	
☒ Verschlüsselung von Notebooks / Tablet	
☒ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen	

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	Organisatorische Maßnahmen
☒ Aktenschredder mind. empfohlene Sicherheitsstufe P-4 (DIN 66399)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichtung mind. Sicherheitsstufe P-6 (DIN 66399)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Richtlinie Informationssicherheit
☒ Zugriffe SSH Verschlüsselt	☒ Arbeitsanweisung Kommunikationssicherheit
☒ zertifizierte SSL Verschlüsselung	☒ 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	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Richtlinie Informationssicherheit
☒ VLAN-Segmentierung	☒ Richtlinie Datenschutz
☒ Kundensysteme logisch getrennt	☒ Arbeitsanweisung Betriebssicherheit
☒ Staging von Entwicklungs-, Test und Produktivumgebung	☒ 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	Organisatorische Maßnahmen
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System (verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren
☒ auf Wunsch des Kunden werden Logfiles pseudonymisiert	☒ 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	Organisatorische Maßnahmen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https – Secure Cloudstores	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Nutzung von Signaturverfahren (fallabhängig)	☒ 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	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle (nach strikten internen Vorgaben)	☒ 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	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup-Konzept
☒ Feuerlöscher Serverraum	☒ Keine sanitären Anschlüsse im Serverraum
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Existenz eines Notfallplans
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV-Anlage und Notrom-Dieselaggregate RZ	☒ Getrennte Partitionen für Betriebssysteme und Daten, wo notwendig
☒ Schutzsteckdosenleisten Serverraum	☒ Richtlinie Informationssicherheit
☒ RAID System / Festplattenspiegelung	☒ Arbeitsanweisung Betriebssicherheit
☒ Videoüberwachung Serverraum	☒ Regelmäßige Tests der Dieselaggregate RZ
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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	Organisatorische Maßnahmen
☒ Backup-Monitoring und -Reporting	☒ Recovery-Konzept
☒ Wiederherstellbarkeit aus Automatisierungs-Tools	☒ 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
	☒ Existenz eines Notfallplans
	☒ Richtlinie Informationssicherheit
	☒ Arbeitsanweisung Betriebssicherheit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutzmanagement

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter	☒ Interner Datenschutzbeauftragter bestellt: Group Data Protection Officer, DPO
☒ Sicherheitszertifizierung nach ISO 27001	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☒ Eine Überprüfung der Wirksamkeit der TOM wird mind. jährlich durchgeführt und TOMs aktualisiert	☒ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
☒ Datenschutzprüfpunkte durchgängig in Tool-gestütztem Risk Assessment implementiert	☒ 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	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DPO und ☒ ISO in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
☒ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung	☒ 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	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Richtline Datenschutz (inkludiert Prinzipien „Privacy by design / default")
☒ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware	☒ 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	Organisatorische Maßnahmen
☒ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support	☒ Arbeitsanweisung Lieferantenmanagement und Lieferantenbewertung
☒ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln 1, 2	☒ 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-, Informationssicherheits- und Risikopolitik** 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 Führung und Steuerung** der Unternehmensgruppe im Rahmen eines **Integrierten Management Systems (IMS)**. Anexia hat in diesem Zusammenhang eine ausgeprägte **Informationssicherheits- und Datenschutz-Querschnittsorganisation** etabliert, um einen umfassenden Schutz ihrer eigenen Unternehmensinformationen- und Daten sowie der Daten ihrer Kunden und Auftraggeber zu schützen. Dabei sind die Funktionen **Information Security Officer (ISO)**, **Data Protection Officer (DPO)**, **Quality Officer (QO)** sowie **Risk Officer (RO)** 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 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 Abschluss einer Auftragsverarbeitungs-vereinbarung (AVV) nach Art 28 DSGVO eingesetzt, mit welcher ihnen alle datenschutzrechtlichen Pflichte 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** (siehe Kapitel 6) 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 der **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