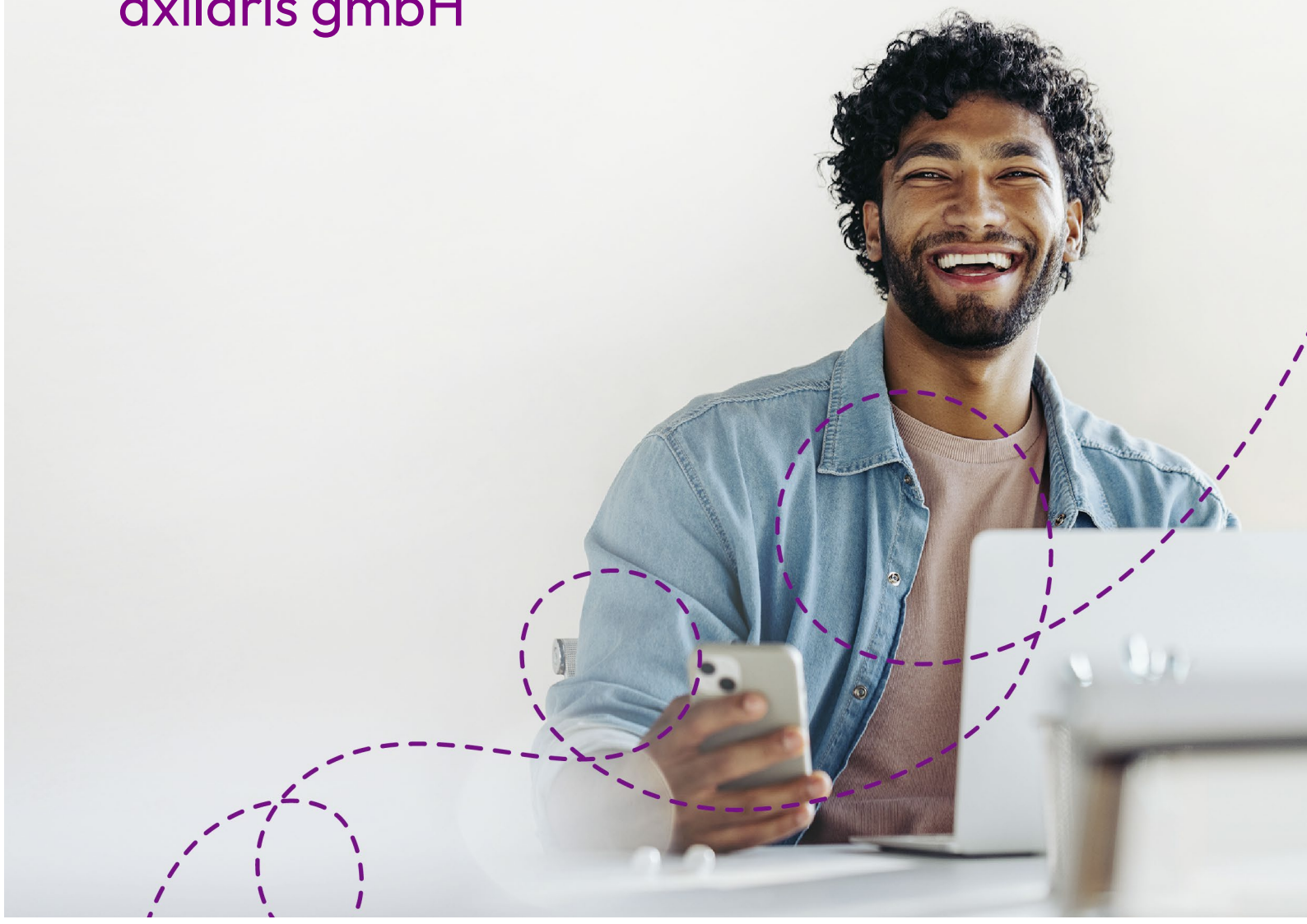
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO der axilaris gmbH



Inhaltsverzeichnis

Allgemeine Informationen 3
Änderungshistorie 3
Allgemeines 4
Vertraulichkeit 4
- Zutrittskontrolle 4
- Zugangskontrolle 4
- Zugriffskontrolle 4
- Trennungskontrolle 5
- Pseudonymisierung 5

Integrität 5
- Weitergabekontrolle 5
- Eingabekontrolle 5
- Verfügbarkeit und Belastbarkeit 6

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 6
- Datenschutz-Management, einschließlich Mitarbeiter- Schulungen 6
- Incident-Response-Management 6
- Datenschutzfreundliche Voreinstellungen 6
- Auftragskontrolle 7

Allgemeine Informationen

DokumentenNr.:	BE_00006
Dokumententyp:	Bericht
Vertraulichkeitsstufe:	intern
Status:	Freigegeben (Approved)
Ansprechpartner/in & Verantwortliche/ r:	Sándor Helbing
Geltungsbereich:	Organisation, Personal
Autor(en):	Gabriela Rose, Sándor Helbing

Aus Gründen der besseren Lesbarkeit wird im Text hauptsächlich die männliche Form für Personen und Personengruppen verwendet. Sie bezieht sich auf Personen jeden Geschlechts.

Änderungshistorie

Version	Veröffentlicht	Geändert von	Kommentar
AKTUELL (v. 9)	2026-01-20 | 07:29	Sándor Helbing	
v. 8	2026-01-19 | 17:40	Sándor Helbing	
v. 7	2026-01-19 | 17:02	Gabriela Rose Sándor Helbing Oliver Hintzsche	

Allgemeines

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO der axilaris GmbH. Es berücksichtigt den internen Datenschutz, den Betrieb der IT Systeme einschließlich Rechenzentrums und Netzwerkinfrastruktur sowie sämtliche Verarbeitungsvorgänge personenbezogener Daten innerhalb der axilaris GmbH.

Die ehemals unter der Firma managedhosting.de GmbH betriebenen Hosting und Infrastrukturdienstleistungen wurden vollständig durch die axilaris GmbH übernommen und werden organisationsintern betrieben. Eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO liegt insoweit nicht vor.

Vertraulichkeit

Zutrittskontrolle

Das Rechenzentrum sowie alle sicherheitsrelevanten Betriebsbereiche der axilaris GmbH sind in unterschiedliche Sicherheitszonen unterteilt. Der Zutritt zu diesen Bereichen ist ausschließlich autorisierten Personen gestattet und erfolgt über personalisierte Zutrittsmedien. Sämtliche Zutrittsereignisse werden protokolliert und regelmäßig überprüft.

Die Rechenzentrumsstandorte unterliegen den Anforderungen eines zertifizierten Informationssicherheitsmanagementsystems nach ISO IEC 27001. Zur Absicherung gegen unbefugten Zutritt bestehen elektronische Zutrittskontrollsysteme, Videoüberwachung sicherheitsrelevanter Bereiche sowie Einbruch und Alarmmeldeanlagen. Die Verarbeitung der hierbei anfallenden Daten erfolgt ausschließlich zu Sicherheits- und Nachweiszwecken. Fremdpersonal erhält Zutritt nur in Begleitung berechtigter Mitarbeiter. Außerhalb der Geschäftszeiten erfolgen zusätzliche Kontrollen durch Sicherheitsdienste.

Zugangskontrolle

Der Zugriff auf IT Systeme und Anwendungen der axilaris GmbH erfolgt über zentrale Authentifizierungs- und Autorisierungskomponenten unter Einsatz eines Identity und Access Management Systems. Die Authentifizierung der Benutzer erfolgt systemabhängig über angebundene zentrale Verzeichnisdienste wie Active Directory oder LDAP sowie gegebenenfalls über systemeigene Benutzerverwaltungen.

Für den Fernzugang sowie für den Zugriff auf besonders schützenswerte, sicherheitskritische oder exponierte Systeme und Funktionen sind starke Authentisierungsmechanismen in Form mehrstufiger Authentifizierungsverfahren implementiert. Die starke Authentisierung erfolgt je nach Systemkontext durch die Kombination aus Wissens und Besitzfaktoren, beispielsweise Passwort und Token oder OTP, oder durch gleichwertige Verfahren starker Authentisierung wie Public Key basierte Authentifizierungsmechanismen.

Zur Reduzierung des administrativen Aufwands und zur Erhöhung des Sicherheitsniveaus werden, wo technisch möglich und organisatorisch sinnvoll, Single Sign On Verfahren eingesetzt, die auf die zentralen Verzeichnisdienste aufsetzen.

Zugriffskontrolle

Die Vergabe, Änderung und Entziehung von Zugangs- und Zugriffsrechten erfolgt zentral über das Identity und Access Management System. Benutzer erhalten ausschließlich Zugriff auf diejenigen Daten und Systeme, die zur Erfüllung ihrer jeweiligen Aufgaben erforderlich sind.

Es erfolgt eine organisatorische und technische Trennung von regulären Benutzerkonten und administrativen Konten. Administrative Tätigkeiten werden ausschließlich über dedizierte Administrationszugänge durchgeführt, die erhöhten Authentisierungs- und Kontrollanforderungen unterliegen. Die vergebenen Zugangs- und Zugriffsrechte werden regelmäßig, mindestens jedoch einmal jährlich, überprüft. Die Ergebnisse dieser Rezertifizierung werden dokumentiert.

Trennungskontrolle

Die Trennung personenbezogener Daten nach unterschiedlichen Verwendungszwecken erfolgt durch eine Kombination aus organisatorischen und technischen Maßnahmen. Hierzu zählen die Trennung von Produktiv und Testsystemen, mandantenfähige Systemarchitekturen, getrennte Datenbanken sowie differenzierte Zugriffsregelungen.

Die Wirksamkeit dieser Trennungsmaßnahmen wird regelmäßig überprüft.

Pseudonymisierung

Sofern dies für den jeweiligen Verarbeitungsvorgang möglich, beauftragt und zweckmäßig ist, werden primäre Identifikationsmerkmale personenbezogener Daten entfernt und durch dynamische Werte ersetzt. Die Zuordnungsinformationen werden getrennt gespeichert und besonders geschützt aufbewahrt.

Integrität

Weitergabekontrolle

Um sicherzustellen, dass personenbezogene Daten ausschließlich an berechtigte interne Stellen weitergegeben werden und nicht unbefugt offengelegt, verändert oder gelöscht werden können, bestehen umfassende organisatorische und technische Maßnahmen.

Die Nutzung von Internet und E-Mail Diensten ist durch verbindliche Richtlinien geregelt und von allen Mitarbeitern schriftlich bestätigt. Personenbezogene Daten dürfen ausschließlich zweckgebunden verarbeitet und übermittelt werden.

Eine Mitnahme von Datenträgern ist grundsätzlich untersagt. Ausnahmen bedürfen einer dokumentierten Genehmigung. Ausgemusterte Datenträger werden sowohl softwaregestützt nach anerkannten Löschverfahren als auch mechanisch zerstört. Elektronische Übermittlungen personenbezogener Daten erfolgen ausschließlich verschlüsselt unter Einsatz zertifikatsbasierter Verfahren oder transportverschlüsselter Verbindungen. Die Identität und Vertrauenswürdigkeit der empfangenden Stelle wird vor der Übermittlung geprüft.

Jeder manuelle Transport personenbezogener Daten wird schriftlich dokumentiert und vom Empfänger gegengezeichnet. Zusätzlich stellen technische Schutzmaßnahmen wie Firewalls, VPN Gateways, Content Filter und Zugriffskontrollmechanismen sicher, dass keine unbefugte Übermittlung erfolgt.

Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten ist nachvollziehbar und revisionssicher ausgestaltet. Die Nachvollziehbarkeit wird abhängig vom jeweiligen System durch Protokollierung auf Applikations-, Datenbank oder Betriebssystemebene sichergestellt. Protokolliert werden insbesondere Benutzerkennung, Zeitpunkt, Art der Änderung sowie das betroffene Datenobjekt.

Administrative Tätigkeiten wie Konfigurationsänderungen, Benutzeranlagen, Rechtevergaben oder Backup Operationen werden gesondert erfasst. Die Protokolldaten sind gegen unbefugte Veränderung geschützt, werden für definierte Zeiträume aufbewahrt und regelmäßig ausgewertet.

Verfügbarkeit und Belastbarkeit

Die kritischen IT Systeme der axilaris GmbH sind unter Berücksichtigung der Wirtschaftlichkeit redundant ausgelegt. Zur Absicherung gegen Ausfälle bestehen Mehrfachauslegungen von Servern, Speichersystemen, Netzwerkkomponenten und Stromversorgung.

Alle relevanten Systeme sind an unterbrechungsfreie Stromversorgungen angeschlossen und durch Überspannungsschutz sowie Netzersatzanlagen abgesichert. Rechenzentrumsbereiche verfügen über automatische Brandmelde und Löschanlagen sowie physische Sicherungsmaßnahmen. Regelmäßige Datensicherungen erfolgen gemäß Datensicherungskonzept unter Berücksichtigung der Kritikalität der Daten.

Notfall und Wiederanlaufpläne stellen sicher, dass die Verfügbarkeit der Systeme nach Störungen oder Ausfällen zeitnah wiederhergestellt werden kann. Die Wirksamkeit dieser Pläne wird regelmäßig getestet und dokumentiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die technischen und organisatorischen Maßnahmen werden regelmäßig überprüft bewertet und an den Stand der Technik angepasst. Grundlage bilden interne Richtlinien, ein Datenschutzleitbild sowie ein etabliertes Informationssicherheitsmanagement.

- Datenschutzleitbild der Sparkassen Finanzgruppe
- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- Bestellung eines betrieblichen Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis/Vertraulichkeit und Bankgeheimnis
- Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- Prüfung/Auditierung der Informationssicherheit (etwa im Rahmen von ISO-Zertifizierung)

Datenschutz-Management, einschließlich Mitarbeiter- Schulungen

Es bestehen verbindliche Prozesse zur Schulung und Sensibilisierung der Mitarbeiter in Datenschutz und Informationssicherheit. Neue Mitarbeiter werden vor Aufnahme ihrer Tätigkeit verpflichtet und regelmäßig fortgebildet.

Ein Verzeichnis von Verarbeitungstätigkeiten wird gemäß Art. 30 DSGVO geführt. Datenschutzfolgenabschätzungen werden durchgeführt, sofern Art Umfang oder Zweck der Verarbeitung dies erfordern.

Incident-Response-Management

Für Datenschutzverletzungen bestehen dokumentierte Incident Response Prozesse, einschließlich Meldewegen gegenüber Aufsichtsbehörden und betroffenen Personen gemäß Art. 33 und 34 DSGVO unter Einbindung des Datenschutzbeauftragten.

Datenschutzfreundliche Voreinstellungen

Systeme und Anwendungen sind datenschutzfreundlich vorkonfiguriert. Es werden nur solche personenbezogenen Daten verarbeitet, die für den jeweiligen Zweck erforderlich sind. Änderungen erfolgen ausschließlich nach dokumentierter Freigabe.

Auftragskontrolle

Grundsätzlich erfolgt die Datenspeicherung und Datenverarbeitung nach den Vorgaben der DS-GVO.

Die axilaris GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt, der für Vor-Ort-Kontrollen verantwortlich ist.

Erfolgt eine Auftragsdatenverarbeitung nach Art. 32 DS-GVO so werden die Einzelheiten zur Auftragskontrolle in einem Vertrag zur Auftragsverarbeitung durch den Auftraggeber festgelegt.

Die Auftragskontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten, der regelmäßig die Einhaltung der vertraglichen Datenschutzanforderungen durch unsere Auftragsverarbeiter überprüft und dokumentiert, um die DSGVO-konforme Verarbeitung personenbezogener Daten sicherzustellen.