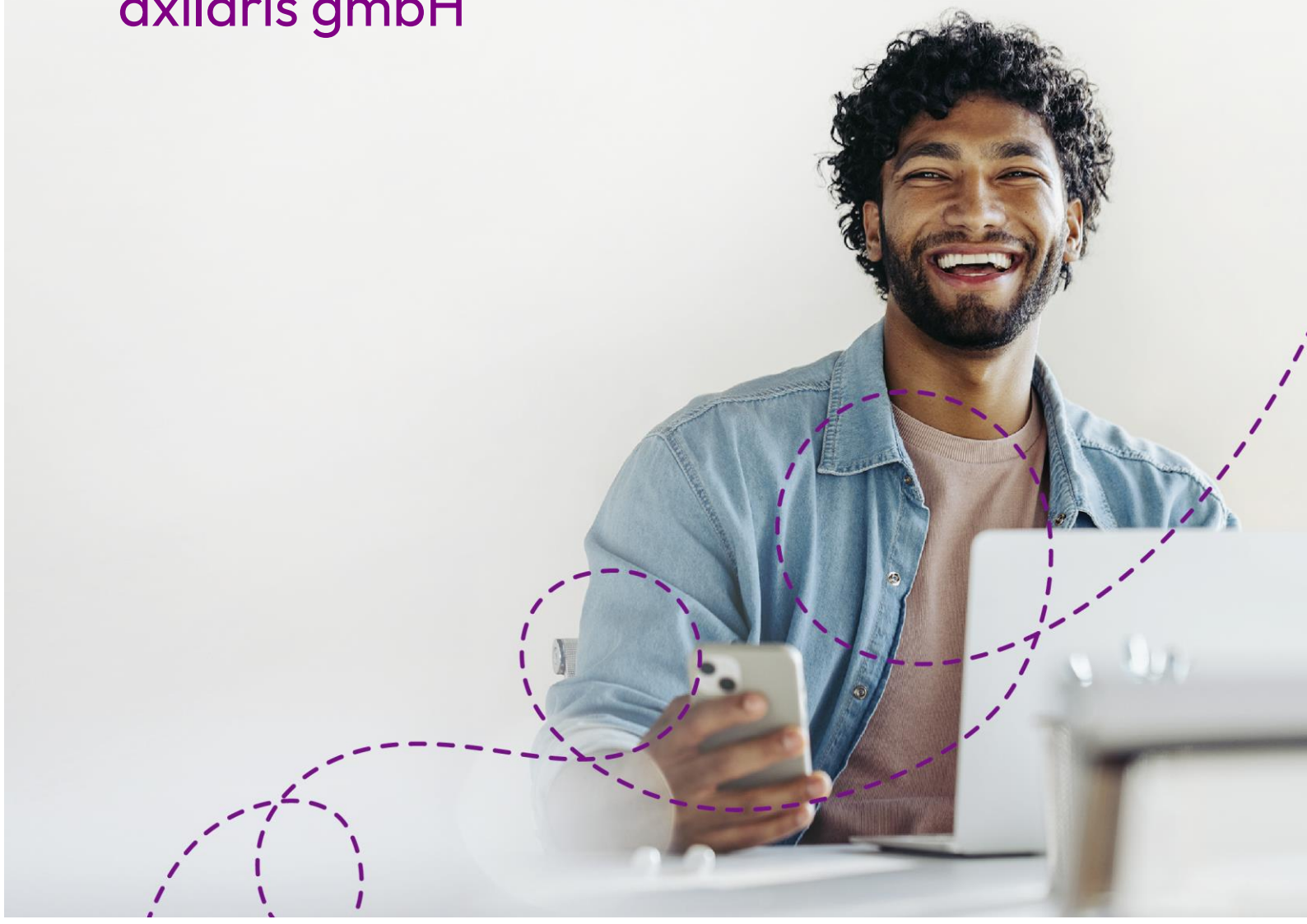
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO der axilaris gmbH



Inhaltsverzeichnis

Allgemeine Informationen

DokumentenNr.:	BE_00006
Dokumententyp:	Bericht
Vertraulichkeitsstufe:	Für den internen Gebrauch
Status:	Freigegeben (Approved)
Ansprechpartner/in & Verantwortliche/ r:	Sándor Helbing
Geltungsbereich:	Organisation, Personal
Autor(en):	Gabriela Rose, Sándor Helbing
Abgelöste Dokumentennummer:	KO_00011

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. 6)	2024-08-21 | 09:01	Sándor Helbing	
v. 5	2024-08-21 | 08:53	Sándor Helbing	
v. 4	2023-06-19 | 13:17	Sándor Helbing	

Allgemeines

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen nach Art. 32 DS- GVO der axilaris GmbH.

Berücksichtigt wurden in diesem Dokument der interne Datenschutz, sowie das Datennetz in den Geschäftsräumen der axilaris GmbH.

Vertraulichkeit

Zutrittskontrolle

Das Rechenzentrum der axilaris GmbH ist aufgrund differenzierter Sicherheitsanforderungen in verschiedene Sicherheitszonen unterteilt und durch organisatorische Maßnahmen gegen den Zutritt nichtberechtigter Personen geschützt. Ein Zutritt zu den Sicherheitszonen ist nur durch die Herausgabe eines Transponders möglich. Der Zutritt zu den Sicherheitszonen wird im Zutrittskontrollsystem überwacht und protokolliert. Der Datenschutzbeauftragte führt vierteljährlich eine gründliche Überprüfung und Auswertung der Zutrittsprotokolle durch, um mögliche Sicherheitsvorfälle frühzeitig zu erkennen und entsprechende Maßnahmen einzuleiten.

Für den Zugang eines Mitarbeiters wird benötigt:

- Name, Vorname
- Bild
- PIN Code
- Raumzonenberechtigungen
- Unterschrift des Mitarbeiters bzw. des Schlüsselverantwortlichen bei Erhalt des Transponders

Fremdpersonal wird der Zutritt in das Rechenzentrum der axilaris GmbH nur in Begleitung eines zutrittsberechtigten Mitarbeiters gewährt.

Außerhalb der Geschäftszeiten wird das Gebäude durch einen Sicherheitsdienst kontrolliert.

Zugangskontrolle

Die Benutzung der zentralen Rechner und Server ist nur mit einer gültigen Benutzerkennung zusammen mit einem gültigen Passwort möglich. Die Protokolle über die Systembenutzung werden regelmäßig von der axilaris GmbH auf fehlgeschlagene Anmeldeversuch hin untersucht.

Die Benutzerverwaltung und deren Zugriffsberechtigungen werden durch Maßnahmen wie

- Passwortvergabe,
- Protokollierung der Passwortvergabe,
- je Nutzer ein eigenes Passwort,
- Protokollierung von Umgehungsversuchen,
- keine Übertragung von Passwörtern im Klartext,

sichergestellt.

Die IT-Systeme können sich nur durch ihr Wissen (gemeinsames Geheimnis) und eventuell durch die Herkunft der Leitung (IP-Adresse) erkennen. Hierzu werden auf den Netzwerkkomponenten (Firewall, Layer 3 Switch) Kommunikationsbeziehungen gepflegt. Die externe Kommunikation über das Internet erfolgt für vertrauliche Informationen immer über ein SSL-Gateway. Die Authentizität ist durch eine 2-Faktor Authentifizierung mit RSA-Token/ per PublicKey und Pin sichergestellt.

Zur Sicherstellung der Sicherheit wird die Zugangskontrolle regelmäßig zu festgelegten Terminen überprüft. Nicht mehr benötigte Zugänge werden identifiziert und durch ein Löschprotokoll dokumentiert und entfernt.

Zugriffskontrolle

Zugriffsmöglichkeiten zur Benutzung eines DV-Systems werden ausschließlich auf die der Zugriffsberechtigung unterliegenden Daten eingeräumt. Dies wird zum einen sichergestellt durch

- funktionelle Zuordnung einzelner Datenendgeräte,
- automatische Prüfung der Zugriffsberechtigung,
- Protokollierung der Systemnutzung und Protokollauswertung,
- sowie einer differenzierten Zugriffsberechtigung auf
  - Dateien und Verzeichnisse,
  - Anwendungsprogramme
  - und der Betriebssystemsoftware.

Das Betriebssystem unterstützt hierbei differenzierte Verarbeitungsmöglichkeiten (Berechtigungen) wie Lesen, Schreiben, Ändern oder Löschen von Dateien oder Verzeichnissen.

Die axilaris GmbH verfügt über Datenträgerarchive zur Verwahrung magnetischer und optischer Datenträger. Diese gehören zur höchsten Sicherheitszone und sind räumlich von anderen Bereichen getrennt und geschützt. Zusätzlich können je nach Schutzbedarf Datenträgerarchive verschlüsselt werden.

Die Datenträger werden mit einer eindeutigen Kennzeichnung versehen. Jede Entnahme eines Datenträgers sowie sein Rücklauf werden protokolliert, sodass jederzeit sein Aufenthaltsort ermittelt werden kann.

Die Vernichtung auszumusternder Datenträger erfolgt gemäß einer Sicherheitsrichtlinie für die Vernichtung von Datenträgern.

Im Rahmen der regelmäßigen Rezertifizierung überprüfen die Produkteigner die Zugriffskontrollen sorgfältig. Ein speziell dafür eingesetztes Tool unterstützt diesen Prozess, um sicherzustellen, dass alle Zugriffsberechtigungen stets aktuell und korrekt sind.

Trennungskontrolle

Die Trennung der Daten nach unterschiedlichem Zweck und deren Verwendung erfolgt durch

- Trennung von Produktiv- und Testsystemen,
- Trennung der Zugriffsregelung,
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung),
- separate Tabellen innerhalb von Datenbanken,
- getrennte Datenbanken,
- Mandantentrennung,
- Dateiseparierung

Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, gesondert aufbewahrt und in der Anwendung durch sich einen sich ändernden Wert, Zeichen oder Zeichenkette ersetzt.

Die Pseudonymisierung personenbezogener Daten wird konsequent angewendet, indem primäre Identifikationsmerkmale entfernt und durch dynamische Werte ersetzt werden, die regelmäßig aktualisiert werden, falls erforderlich.

Integrität

Weitergabekontrolle

Um sicherzustellen, dass personenbezogene Daten nur an die festgelegten Empfänger weitergegeben werden und die Daten nicht unbemerkt verfälscht werden können, wurde in der axilaris GmbH eine Regelung zur Nutzung des Internets und E-Mail-Verkehrs erlassen und durch die Mitarbeiter schriftlich bestätigt.

Grundsätzlich besteht ein Verbot der Mitnahme von Datenträgern für alle Mitarbeiter der axilaris GmbH. Ausgemusterte Datenträger werden sowohl per Softwaretool einem speziellen Löschverfahren unterzogen, als auch mechanisch zerstört.

Optische Datenträger werden gemäß einer Sicherheitsrichtlinie bei der Entsorgung geschreddert.

Müssen personenbezogene Daten ausnahmsweise an vertrauenswürdige Personen elektronisch übermittelt werden, so erfolgt dies ausschließlich zertifikatsbasierend (PGP/SMIME) und verschlüsselt, wobei die Vertraulichkeit der Gegenstellen vor dem Datentransport geprüft wird.

Jeder manuelle Transport von personenbezogenen Daten wird schriftlich protokolliert und vom Empfänger gegengezeichnet. Zum Transport werden die Datenträger, die personenbezogene Daten enthalten, grundsätzlich verschlüsselt.

Umfassende technische Maßnahmen wie Firewall, VPN-Gateway, Content Filter und Access Control Lists stellen sicher, dass keine Daten in unbefugte Hände gelangen. Maßnahmen zur Datenverschlüsselung sorgen während der Übermittlung der Daten dafür, dass diese nicht gelesen oder verändert werden können.

Eingabekontrolle

Die Eingabe, Änderung und Löschung von Daten kann durch Protokollierung in den Anwendungen selbst oder durch Protokollierung auf Betriebssystemebene (Datenbank-Logs) nachvollzogen werden.

Verfügbarkeit und Belastbarkeit

Die kritischen IT-Systeme der axilaris GmbH sind unter Beachtung der Wirtschaftlichkeit redundant ausgelegt.

Alle benötigten IT-Systeme der axilaris GmbH sind an die unterbrechungsfreie Stromversorgung (USV) sowie Überspannungsfilter angeschlossen, welche mit einer Netzersatzanlage (NEA) gekoppelt ist.

Es gibt eine automatische Brandmeldeanlage für das Rechenzentrum unter Einschluss der Zellen.

In den Rechenzentren sind am jeweiligen Standort Löschanlagen installiert, welche jährlich einem VdS-Test unterzogen werden.

Im Rechenzentrum sind Einbruchsmeldeanlagen für die Außenhautüberwachung, Bewegungsmelder für die Fallenüberwachung und eine Videoanlage installiert. Die Videoüberwachung ist ausschließlich zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Geltendmachung von Rechtsansprüchen, insbesondere zum Zwecke der Beweissicherung vorhanden. Es existieren entsprechende Prozesse zur Abarbeitung von Vorfällen unter Beteiligung des Sicherheitsdienstes.

Notfall- und Wiederanlaufpläne der kritischen IT-Systeme und Anwendungen unterstützen eine schnelle Wiederherstellung der Arbeitsfähigkeit bzw. der Produktion. Die Verfügbarkeit und Belastbarkeit der kritischen IT-Systeme werden durch regelmäßige Tests der Notfall- und Wiederherstellungspläne sowie durch kontinuierliche Wartung der redundanten Infrastruktur sichergestellt, um eine schnelle Wiederherstellung im Falle von Störungen oder Ausfällen zu gewährleisten.

Regelmäßige Sicherungen der Datenbestände erfolgen gemäß Datensicherungskonzept, welches sich an der Kritikalität der Daten orientiert:

- wöchentliches Backup der Daten,
- tägliches Backup der Daten,
- Plattenspiegelung (RAID),
- Backup Standort.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management, einschließlich Mitarbeiter- Schulungen

- 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)

Die regelmäßige Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen erfolgt regelmäßig um sicherzustellen, dass alle Prozesse den aktuellen Anforderungen entsprechen und kontinuierlich verbessert werden.

Incident-Response-Management

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

Datenschutzfreundliche Voreinstellungen

- administrative gehärtete Systeme ohne Updatemöglichkeiten

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.