adventics GmbH

Büro Haar bei München
Münchener Str. 23a
85540 Haar bei München

Tel. +49 (89) 4444 33 111

Email info@adventics.de
Web www.adventics.de

Stand September 2023

Technische und organisatorische Sicherheitsmaßnahmen der adventics GmbH

Gesellschaft / Standort

Die nachstehenden technischen und organisatorischen Sicherheitsmaßnahmen beziehen sich auf:

- adventics GmbH

  Münchener Str. 23A

  85540 Haar bei München, Deutschland
- adventics GmbH

  Seidlgasse 34

  1030 Wien, Österreich

A. Art. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die adventics GmbH geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

B. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

B.1. Zutrittskontrolle

Definition

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

B.1.1. Bürogebäude

- Die Büroräume der adventics GmbH in Deutschland befinden sich in der Münchner Str.23A, 85540 Haar bei München.
- Die Büroräume der adventics GmbH in Österreich befinden sich in der Seidlgasse 34, 1030 Wien.
- Die Büroräume sind mit einem mechanischen Schließsystem versehen.
- Die Schlüsselausgabe an Mitarbeitern wird protokolliert.
- Die Schlüsselvergabe findet durch die Geschäftsleitung statt.

B.1.2. Besucherregelungen

- Per Zutrittsregelung dürfen sich Besucher nur in ständiger Begleitung mit dem zuständigen Ansprechpartner in den Büroräumlichkeiten bewegen.

B.1.3. Zutritt Serverraum

- Die Serverräume der adventics, auf denen personenbezogenen Daten verarbeitet werden, befinden sich in Europa. Die Server werden gehostet durch:
  - Microsoft Azure EU Data Center Europe West/ Niederlande

    Das Azure Data Center Europe West hat folgende Zertifizierungen: CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001 PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight | BIR 2012 | AFM + DNB NEN-7510

    https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure
  - Zoho EU Data Center Amsterdam, Niederlande

    Das Zoho Data Center in den Niederlanden hat folgende Zertifizierungen: ISO 27001 ISO 22301 SOC 2 TYPE IIISO 50001 PCI DSS

B.2. Zugangs- und Zugriffskontrollmaßnahmen

Definition

Maßnahmen, die sicherstellen, dass

- Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können,
- der Versuch des unbefugten Zugangs nicht unbemerkt bleibt,
- die zur Benutzung der Datenverarbeitungsanlagen befugten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und unbefugtes Lesen, Kopieren, Ändern verhindert wird,
- der Versuch des unbefugten Zugriffs nicht unbemerkt bleibt.

B.2.1. Zugangsberechtigungen

- Definierter Freigabeprozess, welcher Mitarbeiter auf welche personenbezogene Daten Zugang hat.
- Vergabe bzw. Zugriffsberechtigungen werden protokolliert.
- Jeder Mitarbeiter erhält ein personalisiertes Benutzerkonto.
- Jeder Mitarbeiter muss sich bei jeden Log-In über einer 2-Faktor-Authentifizierung identifizieren.
- Es existiert ein Passwort-Parameter:
  - Das Passwort enthält mindestens 8 Zeichen,
  - Passwörter beinhalten jeweils Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen,
  - Passwörter dürfen nicht leicht zu erraten sein (Geburtsdatum),
  - Trivialpasswörter (1111) dürfen nicht verwendet werden,

- Bereits genutzte Passwörter dürfen nicht erneut verwendet werden.
- Das System zwingt zur Einhaltung der Passwortvorgabe.
- Bei Inaktivität schaltet sich der Bildschirm nach 5 Minuten ab.
- Sollte der Verdacht auf Kompromittierung bestehen, muss das Passwort unmittelbar durch die 2-Faktor- Authentifizierung geändert werden.
- Die Anmeldeversuche sind begrenzt und bleiben bis zur manuellen Aufhebung durch die IT auch gesperrt.
- Bei Fernzugängen erfolgt die Identifizierung der Mitarbeiter ebenfalls über eine 2-Faktor-Authentifizierung.
- Die Anmeldeversuche bei Fernzugriffen sind begrenzt und bleiben bis zur manuellen Aufhebung durch die IT auch gesperrt.

B.3. Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten

Definition

Maßnahmen, die die Umsetzung von geeigneten technischen und organisatorischen Maßnahmen auch auf mobilen Datenträgern und Endgeräte sowie auf Papier-Unterlagen gewährleisten.

B.3.1. Papierunterlagen

- Vertrauliche und geheime Informationen in Papierform sind ausschließlich über den im Unternehmen zur Verfügung gestellten Schreddern (Sicherheitsstufe P4) zu entsorgen.

B.3.2. Mobile Datenträger und mobile Endgeräte

- Es werden Datenträger für den Austausch von Daten genutzt. Datenträger von unbekannter Herkunft dürfen nicht zusammen mit Firmenhardware verwendet werden.
- Die zum Datenaustausch genutzten mobilen Datenträger, wie z. B. USB-Sticks sind auf der Festplatte zu verschlüsseln.
- Der Gebrauch von privaten mobilen Endgeräten ist untersagt.
- Die Entsorgung von mobilen Endgeräten und Datenträgern erfolgt durch die IT-Abteilung.

B.3.3. Maßnahmen zur sicheren Datenübertragung

Definition

Maßnahmen, die sicherstellen, dass

- Daten bei der elektronischen Übertragung oder während des Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Ein Transport von physischen Datenträgern mit personenbezogenen Daten zu einem Aktenvernichtungsdienstleiter nur in geschlossenen Behältnissen und in geschlossenen Fahrzeugen durchgeführt wird, so dass keine Daten verloren gehen können.

B.3.4. Weitergabekontrolle

- E-Mails werden per TLS übermittelt.
- Betrieb und Einsatz eines FTP-Servers, über den das File-Sharing und der sichere bzw. verschlüsselte Versand von Dateien gewährleistet ist.
- Datenträger, die für den Austausch von Daten genutzt werden, sind verschlüsselt.
- Die Schlüssel bzw. Zertifikate werden durch die hauseigene IT verwaltet.

C. Maßnahmen zur Sicherstellung der Verfügbarkeit

Definition

Maßnahmen zur Datensicherung (physikalisch / logisch) gegen zufällige Zerstörung oder Verlust.

C.1. Serverraum

- Bei den Serverraum handelt es sich um einen innenliegenden Raum ohne Fenster.
- Der Serverraum ist mit einer feuerhemmenden Zugangstür aus Massivwand geschützt.
- Der Serverraum ist an die Brandmeldezentrale angeschlossen.
- Der Serverraum ist sowohl mit einem Löschsystem (CO2 Löscher und Halon/ Argon Löschanlage) als auch mit einer Klimatisierung ausgestattet.
- Unterbrechungsfreie Stromversorgung, welche zusätzlich durch ein Dieselaggregat abgesichert und deren Funktionalität regelmäßig getestet wird.

C.2. Backup- und Notfall-Konzept, Virenschutz

- Dokumentiertes Backup-Konzept.
- Regelmäßiges Testen des Backup-Konzeptes.
- Die Durchführung und Dokumentation des Backup Checks findet in regelmäßigen Abständen aber mindestens zweimal im Monat statt.
- Die Durchführung und Dokumentation der Backup Checks werden durch die externen Dienstleister Microsoft Azure und Zoho durchgeführt.
- Die regelmäßige Erstellung von Backups erfolgt auf dem Online Cloud Speicher der genannten externen Dienstleister.
- Die Lagerung der Backups erfolgt in einem vom primären Server getrennten Abschnitt.

C.2.1.1. Change- und Patchmanagement

- Dokumentation des Change- und Patchmanagements, welches durch die hauseigene IT zu verantworten ist.

C.2.1.2. Notfallvorsorgekonzept

- Dokumentation eines Notfallvorsorgekonzeptes mit genauen Handlungsvorgaben.

C.3. Virenschutz

- Alle Server und Clients sind mit einem Virenschutz versehen, welcher stetig von der hauseigenen IT aktualisiert wird. Es dürfen grundsätzlich keine Rechner ohne aktuellen Virenschutz betrieben werden.

C.4. Netzanbindung

- Die gesamte Netzanbindung wird von der hauseigenen IT betrieben und ist bezüglich der einzelnen Standorte nicht redundant miteinander verbunden.

D. Pseudonymisierung/Verschlüsselung, Art. 32 Abs. 1 lit. a DSGVO

Definition

Die Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO) gewährleistet, dass Identifikationsmerkmale personenbezogener Daten, sofern dies zum Schutz der betroffenen Personen erforderlich ist oder aus datenschutzrechtlicher Sicht geboten ist, bestimmter oder bestimmbarer Personen durch Kennzeichen ersetzt werden und daher die Zuordnung zur betroffenen Person nicht ohne zusätzliche Informationen möglich ist. Folglich können Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

D.1. Einsatz von Pseudonymisierung

- Sofern möglich, werden Daten pseudonym verarbeitet.
- Soweit Daten im Rahmen der beauftragten Verarbeitung analysiert werden, findet eine datenschutzgerechte Pseudonymisierung oderAnonymisierung statt. Weiterhin ist eine Pseudonymisierung von Daten im Gesamtprozess insofern gewährleistet,dass auf scanbaren Zutrittsausweisen der Besucher und Aussteller („Badges“) lediglich eine eindeutige, i.d.R. nicht fortlaufende Nummer aufgedruckt bzw. im 1D oder 2D Barcode codiert, die erst im Rahmen der verschlüsselten Kommunikation der Scan2Lead Frontend-Geräte mit den Backend-Systemen mit den Personendaten des jeweiligen Besuchers zusammengeführt wird.
- Die Zuordnung und Speicherung von einzelnen Daten erfolgen in getrennt Systemen voneinander.

D.2. Einsatz von Verschlüsselung

- Sofern möglich, sind Daten verschlüsselt zu verarbeiten. Dies ist Einzelfall- und projektabhängig zu beurteilen.
- Die Kommunikation zwischen den Frontend-Geräten der Scan2Lead Anwender und den Backend-Systemen findet ausschließlich unter Einsatz gängiger Verschlüsselungsverfahren statt.

E. Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen - Art. 32 Abs. 1 lit. b, c, d DSGVO

E.1. Durchführung von Systemaudits

- Systemaudits zur Überprüfung der bestehenden Systeme und ob diese funktionieren.
- Sollten sich Abweichungen bzw. Nicht-Konformitäten ergeben, werden diese in der Risikobewertung aufgenommen und entsprechende Gegenmaßnahmen eingeleitet.
- Stetige Überprüfung und Dokumentation der Ergebnisse.

E.1.1. Datenschutzmanagement

- Bestellung eines betrieblichen Datenschutzbeauftragten
- Verpflichtung zur Einhaltung des Datenschutzes nach Maßgabe der DSGVO
- Information der Beschäftigten zu den Themen Datenschutz und Datensicherheit durch Schulungen und schriftlichen Erläuterungen (Anhang zur Verpflichtungserklärung)
- Durchführung von Präsenzschulungen sowie E-Learnings (z.B. bei Einstellung) zu datenschutzrechtlichen Themen
- Abschluss von Verträgen zur Auftragsverarbeitung gemäß Art. 28 DSGVO
- Weitergabe der Verpflichtungen aus dem schriftlichen Vertrag zur Auftragsverarbeitung an Unterauftragnehmer
- Richtlinien und Checklisten zur Beauftragung von Dienstleistern
- Kontrolle der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Information des Auftraggebers bei Fehlern/ Unregelmäßigkeiten in der Datenverarbeitung
- Erläuterungen und Richtlinien zu datenschutzrechtlichen Themen und Vorgaben aus der DSGVO (z.B. Umgang mit Betroffenenanfragen / Vorgehen im Falle einer „Datenpanne“ etc.).

E.1.2. Dokumentation

- Die getroffenen Maßnahmen werden kontinuierlich überprüft und bei Erforderlichkeit überarbeitet.