



TOM-Verzeichnis der aiiio GmbH

Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten nach §32 EU Datenschutz Grundverordnung.

Verantwortlicher:

aiio GmbH
im Folgenden als „aiio“ bezeichnet.

Die Beschreibung der Maßnahmen bezieht sich auch auf Einrichtungen an der Betriebsstätte:
Klausener Str. 10a, 39112 Magdeburg

Verantwortliche verfügungsberechtigte Vertreter (Haftende/r) von aiiio:
Dr. Christian Graup, Knut Köchli, Jobst von Heintze, Lars Bandler

Zum Beauftragten für den Datenschutz ist benannt:

Frau Bettina Pump
LGD Datenschutz GmbH
Rogätzer Straße 8
39106 Magdeburg
Telefon: 0391 5568632-2
E-Mail: datenschutz@lgd-data.de

1. Technische und organisatorische Maßnahmen

Gemäß Arti. 32 DS-GVO, werden durch aiio die technischen und organisatorischen Maßnahmen zur Sicherstellung und Einhaltung des Datenschutzes im Sinne des Gesetzes festgelegt.

2. Innerbetriebliche Organisation

Aiio gestaltet seine innerbetriebliche Organisation derart, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei werden insbesondere Maßnahmen bereitgestellt, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, ein adäquates Datenschutzniveau zu gewährleisten.

3. Notwendige, einzuhaltende Kontrollmechanismen:

Die von aiio getroffenen Maßnahmen wurden im Hinblick auf die Sicherstellung der in den anzuwendenden gesetzlichen Vorschriften verankerten Kontrollebenen konzipiert.

Diese sind:

Gemäß Art. 32 DS-GVO „Sicherheit der Verarbeitung“:

- 1) 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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
 - a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
 - b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- 2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von, beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
- 3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
- 4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Technische und organisatorische Maßnahmen die der Pseudonymisierung oder Verschlüsselung gem. Art. 32, Satz 1 lit. a DSGVO dienen:

Im Umfeld der Geschäftstätigkeit der aiio GmbH existiert kein Vorgang, der eine Pseudonymisierung verlangt oder notwendig erscheinen lässt.

- Jeder Zugriff auf aiio-Systeme erfolgt ausschließlich über transportverschlüsselte Kanäle und Mechanismen. Alle Datentransfers gegenüber allen Systemen, die verschlüsselten Transfer unterstützen, erfolgen verschlüsselt.

Technische und organisatorische Maßnahmen die der Vertraulichkeit, Verfügbarkeit, Belastbarkeit und Integrität, gem. Art. 32, Satz 1 Lit. b DSGVO, dienen:

- Datenträger unterliegen einem dokumentierten Kommissionierungs- und Dekommissionierungsprozess.
- Es werden ausschließlich zertifizierte Dienstleister zur Datenträgervernichtung eingesetzt.
- Alle Dienstleister unterliegen einem strengen Auswahlverfahren.
- Bei Vertragsschluss ist eine der beauftragten Leistung entsprechende Datenschutzvereinbarung obligatorisch.
- Alle aiio-Mitarbeiter sind zur Verschwiegenheit verpflichtet. Die Rechtsgrundlagen der Verschwiegenheitsverpflichtung unterliegen einem dokumentierten, regelmäßigen Sensibilisierungsprozess.
- Alle aiio-Mitarbeiter werden permanent zu Datenschutz und Informationssicherheit geschult und sensibilisiert. Zum Umgang mit Daten und Datenverarbeitungsanlagen findet ein regelmäßiges, dokumentiertes Schulungs- und Sensibilisierungsprogramm Anwendung.
- Zutritt zu den aiio- Räumlichkeiten unterliegt einem dokumentierten Zugangskontrollprozess. Alle Besuche betriebsfremder Personen werden dokumentiert.
- Alle Netzwerkinfrastrukturkomponenten unterliegen einem dokumentierten Aktualisierungsprozess sowie einem dokumentierten Inventarisierungsverfahren.
- Es ist eine umfangreiche Firewall-Appliance in Betrieb, die alle Zugriffe von außen auf die Netzwerkinfrastruktur absichert.
- Es existieren getrennte WLAN-Strukturen für Gäste und interne aiio-Ressourcen (Mitarbeiter und Devices)
- Die logische Trennung von Datenbeständen unterschiedlicher Zwecke oder Umgebungen ist durchgängig sichergestellt.
- Zur Verarbeitung personenbezogener Daten sind prozessbezogene Verfahren etabliert. Datenzugriffsberechtigungen in allen Systemen folgenden Grundsätzen der „Datensparsamkeit“ und Zweckmäßigkeit, entsprechend den Aufgaben der jeweiligen Personen und Personengruppen. Diese werden durch ein umfangreiches Rollen- und Rechtekonzept realisiert.
- Unterbeauftragte Lieferanten werden mittels einer auf die Verarbeitung zugeschnittene Datenschutzvereinbarung (Auftragsverarbeitung oder gemeinsame Verantwortlichkeit) auf ein angemessenes Datenschutzniveau verpflichtet.
- Alle Zugriffe auf öffentlich erreichbare Systeme erfolgen ausschließlich mittels verschlüsselten Transfers.
- Alle Computersysteme sind mit einem mehrstufigen Virenschutzsystem versehen.
- Alle im Unternehmensumfeld verwendeten Browser werden gemäß der jeweiligen Herstellervorgaben gehärtet.
- Alle Datenbestände unterliegen einem mehrstufigen Backup und Restore Verfahren, das regelmäßig auf Zuverlässigkeit geprüft wird.
- Änderung und Aktualisierung von Systemen oder Diensten werden gemäß definierten Prozessen durchgeführt und dokumentiert.

Technische und organisatorische Maßnahmen die der Wiederherstellbarkeit, gem. Art. 32, Satz 1 Lit. c DSGVO dienen:

- Alle Datenbestände unterliegen einem mehrstufigen Backup und Restore Verfahren, das regelmäßig auf Zuverlässigkeit geprüft wird.

Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32, Satz 1 Lit. d DSGVO dienen:

- Alle technischen und organisatorischen Maßnahmen unterliegen einer regelmäßigen Überprüfung auf Einhaltung und Wirksamkeit durch dafür qualifizierte Mitarbeiter des Verantwortlichen und im notwendigen Einzelfall durch externe Prüfende.
- Die Prüfergebnisse werden dokumentiert.

4. Übersichts-Checkliste TOM

4.1 Vertraulichkeit Art. 32 Abs. 1 lit. b DSGVO

4.1.1 Zutrittskontrolle

Eine Zutrittskontrolle soll Unbefugten den Zutritt zu Räumen bzw. Orten in denen personenbezogene Daten archiviert sind bzw. verarbeitet werden, verwehren.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Alarmanlage	☒	Personenkontrolle beim Empfang
☒	Automatisches Zugangskontrollsystem (Transponder)	☒	Schlüsselregelung/Schlüsselbuch
☒	Sicherheitsschlösser	☒	Sorgfältige Auswahl von Sicherheitspersonal
		☒	Videoüberwachung der Zugänge
		☒	Sorgfältige Auswahl von Reinigungspersonal

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die Verhinderung der unbefugten Nutzung von Anlagen gemeint.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Authentifikation mit Benutzer und Passwort	☒	Benutzerberechtigungen verwalten für Entwicklung, SharePoint und O365
☒	Einsatz von Anti-Viren-Software	☒	Erstellen von Benutzerprofilen
☒	Einsatz von Firewalls	☒	Passwortvergabe/Passwortregeln
☒	Einsatz von VPN-Technologie		
☒	Zwei-Faktor-Authentifizierung		
☒	Verschlüsselung von Datenträgern		
☒	Verschlüsselung von Smartphones		
☒	Kennwortverfahren (Sonderzeichen, Wechsel)		
☒	Automatische Sperrung (Pausenschaltung) 3 min.		

4.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden pb Daten zugreifen können, und dass pb Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Einsatz von Aktenvernichtern	☒	Anzahl der Administratoren auf das Notwendigste reduzieren
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten	☒	Erstellung eines Berechtigungskonzepts (Rollen)
☒	Verschlüsselung von Datenträgern	☒	Passwortrichtlinie inkl. Länge
☒	Active Directory unterstützte Zugriffe (Single-Sign-On)	☒	Verwaltung der Benutzerrechte durch Systemadministratoren
	Sammelbehälter. f. ext. Vernichtung	☒	Regelung für den Einsatz privater Datenträger (Verbot)

4.2 Integrität Art. 32 Abs. 1 lit. b DSGVO

Der Begriff „Integrität“ bedeutet, dass die unerkannte Veränderung von pb Daten nicht möglich sein soll. Im Gegensatz zu der Vertraulichkeit, die sich mit der Berechtigung der Datenänderung beschäftigt, soll bei der Integrität eine die Korrektheit der pb Daten sowie eine korrekte Funktionsweise des Systems bestehen. Somit liegt der Fokus der Integrität auf der Nachvollziehbarkeit von Datenänderungen.

4.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass pb 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 von pb Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen		Organisatorische Maßnahmen	
☒	Einrichtung von VPN-Tunneln	☒	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen
		☒	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
		☒	Verpflichtung auf das Datengeheimnis

4.2.2 Eingabekontrolle

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

Technische Maßnahmen		Organisatorische Maßnahmen	
		☒	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
		☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
		☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4.2.3 Auftragskontrolle

Die Auftragskontrolle greift, wenn personenbezogenen Daten im Auftrag von Dritten verarbeitet werden. Zielsetzung ist, dass pb Daten, die einem autorisierten Subunternehmer übermittelt

werden, sowohl gemäß den Bedingungen des Auftraggebers als auch gemäß den Datenschutzbestimmungen verarbeitet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
		☒	Schriftliche Weisungen an den Auftragnehmer (AV-Vertrag)
		☒	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
		☒	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
		☒	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren
		☒	Definierte Vorgehensweise der Vertragsbeendigung

Dieses Dokument wurde elektronisch erstellt und ist ohne Unterschrift gültig.