Anlage 2 – Sicherheit der Verarbeitung – Stand der Technik - TOM

Technische & Organisatorische Maßnahmen

der **Myosotis GmbH**

Zur Erfüllung unserer gesetzlichen Verpflichtungen aus Art. 32 DSGVO, sowie § 34 BDSG (neu) haben wir, die Myosotis GmbH, folgende technische und organisatorische Maßnahmen implementiert, um die Sicherheit der Verarbeitung von personenbezogenen Daten zu gewährleisten.

1.Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(1.1) Schutzmaßnahmen der Zutrittskontrolle:

Die Myosotis GmbH stellt sicher, dass nur autorisierte Personen Zutritt zu den Räumlichkeiten und den darin befindlichen Datenverarbeitungssystemen haben. Das Büro ist außerhalb der Geschäftszeiten geschlossen, während der Geschäftszeiten erfolgt eine visuelle Kontrolle. Nur autorisierte Mitarbeiter haben eine persönliche Ausweiskarte mit Zugangsfunktion.

(1.2) Schutzmaßnahmen der Zugangskontrolle:

Bei der Myosotis GmbH hat jeder Mitarbeiter über einen eigenen Mitarbeiterzugang zu den Systemen der Myosotis GmbH. Die Zugangsrechte beschränken sich dabei auf die Verantwortlichkeiten des jeweiligen Mitarbeiters bzw. Teams. Weitere Dritte, z.B. im Rahmen einer Fernwartung, greifen nicht auf die Systeme zu.
Die Myosotis GmbH arbeitet mit Google Drive zusammen. Daher sind alle Daten in der Cloud und nur über die E-Mail-Adresse und das Passwort der Mitarbeiter zugänglich.
Die Myosotis GmbH hat darüber hinaus eine Regelung zur Erstellung von Passwörtern. Dies garantiert eine höhere Sicherheit für die Systeme.
Passwörter müssen die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen lang
- Mindestens 1 Großbuchstabe
- Mindestens 1 Kleinbuchstabe
- Mindestens 1 Zahl
- Mindestens 1 nicht-alphanumerisches Zeichen

Die Systeme der Myosotis GmbH sind durch Firewalls geschützt, die standardmäßig alle eingehenden Verbindungen ablehnen. Es werden nur die durch die Ausnahme definierten Verbindungstypen akzeptiert.

(1.3) Schutzmaßnahmen der Zugriffskontrolle:

Die Myosotis GmbH hat folgende Maßnahmen ergriffen, um sicherzustellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur gemäß ihrer Zugangsberechtigung auf die Daten zugreifen können und, dass personenbezogene Daten während der Verarbeitung und Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Alle auf dem Server gespeicherten Informationen werden über HTTPS TLS1.2 gesendet, einschließlich aller Arten von Medien. Eine Verschlüsselung auf Anwendungsebene ist im Allgemeinen nicht vorhanden.

- Die Dateien im Mediendatei-Speicher werden unverschlüsselt auf Anwendungsebene gespeichert, aber auf Festplattenebene verschlüsselt.
- Passwörter werden als Hash-Werte gespeichert.
- Alle Server und Dienste der Myosotis GmbH unterliegen einer ständigen Überwachung.
- Der Umfang der Berechtigungen ist jeweils auf das für die Erfüllung von Aufgaben oder Funktionen (logistisch, chronologisch usw.) erforderliche Minimum beschränkt.
- Autorisierte Personen haben nur Zugriff auf die Daten, für die sie berechtigt sind. Es erfolgt eine Berechtigungsprüfung durch einen Identifikationsschlüssel-
- Um den Zugriff auf Kundendaten im Fehlerfall zu verhindern, werden alle Kundendaten auf separaten Servern/Virtual Machines/Datenbanken gespeichert.

(1.4.) Schutzmaßnahmen der Trennungskontrolle:

Zur Trennung von Daten führt die Myosotis GmbH eine logisch getrennte Datenverwaltung durch, sodass es nicht zu einem versehentlichen Auslesen von Daten durch unberechtigte Personen kommen kann.

Myosotis wird die Daten innerhalb der myo APP nicht für andere Zwecke als die Bereitstellung des myo APP-Dienstes verwenden. Die Daten werden in einer mandantenfähigen Architektur gespeichert (siehe Architekturbeschreibung oben), es gibt keine Schnittstellen zur Datenextraktion für z. B. Marketingzwecke.

(1.5) Pseudonymisierung

Klardaten werden nur verwendet, wenn dies zwingend zur Erreichung eines fest definierten Zwecks unabdingbar ist (z.B. Vertragsabwicklung).

2. Integrität
(2.1.) Schutzmaßnahmen der Weitergabekontrolle:

Bei der Myosotis GmbH werden alle Daten cloudbasiert verarbeitet und übertragen. Die Spezifikation der zur Verlegung und/oder zum Transport berechtigten Personen wird derzeit vom Damir Palinic (CTO) auf Produktebene und vom Jasper Böckel / Felix Kuna Management auf der operativen Seite und von Leonore Merck auf der CRM-Seite durchgeführt.

(2.2.) Schutzmaßnahmen der Eingabekontrolle:

Alle Datenübertragungen zu den Cloud-Systemen und zwischen den Komponenten der Cloud-Systeme werden mit dem Protokoll https verschlüsselt.
Das Recht auf Datenübermittlung wird durch Rollen und Rechte gesteuert, die vom CTO zum Zeitpunkt der Überprüfung gewährt werden.

(3) Schutzmaßnahmen der Verfügbarkeits-Belastbarkeitskontrolle:

Kundendatenbanken werden mit dem AWS-Backup-Service gesichert, der Datenbankänderungen der letzten Woche speichert. AWS ermöglicht es den Zustand der Datenbank ab einem bestimmten Zeitpunkt in diesem Zeitraum wiederherzustellen. Backups können auch für eine dauerhafte Aufbewahrung gekennzeichnet werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO
(4.1.) Datenschutzmanagement:

Ein externer Datenschutzbeauftragter wurde bestellt, der eng in die Entwicklung aller datenschutzrechtlich relevanten Prozesse eingebunden ist.

Es erfolgen regelmäßige Schulungen im Datenschutzrecht.

Mitarbeiter werden auf das Datengeheimnis verpflichtet.

Ein Datenschutzmanagementkonzept wurde erstellt und wird regelmäßig überprüft und evaluiert.

(4.2.) Incident-Response-Management:

Im Falle einer Datenpanne existieren Regeln, welche Prozesse in diesem Fall einzuleiten sind und in welcher Form die Aufsichtsbehörden informiert werden.

In der entsprechenden Prozessbeschreibung wurden die Verantwortlichkeiten festgelegt, der technische Ablauf zur Beseitigung der Datenpanne wurde definiert und der Kommunikationsweg zu den Aufsichtsbehörden beschrieben, so dass eine Information der Aufsichtsbehörden binnen 72 Stunden ohne weiteres möglich ist.

(4.3.) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):

Bei der Entwicklung jeder Technologie oder jedes neuen Produktes wird von vornherein ein Privacy-by-Design-Ansatz verfolgt. Es wird von vornherein das Ziel verfolgt, die Menge der zu erhebenden Daten zu minimieren und den Umfang der Datenverarbeitung zu reduzieren

Leicht zugängliche Datenschutzerklärungen sorgen für Transparenz. Auf sämtlichen Transportwegen sind alle Daten verschlüsselt.

(4.4.) Auftragskontrolle

Sämtliche Auftragnehmer sind unter Sorgfaltsgesichtspunkten ausgewählt worden.

Mit sämtlichen Auftragnehmern werden Auftragsverarbeitungsverträge abgeschlossen.

Wirksame Kontrollrechte werden gegenüber dem Auftragnehmer vertraglich vereinbart.

Angemessene technische und organisatorische Maßnahmen beim Auftragnehmer werden analysiert und bewertet und sofern erforderlich regelmäßig überprüft.