Technische und Organisatorische Maßnahmen (TOM) - Übersicht

i.S.d. Art. 32 DSGVO

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Die avy health GmbH hat die folgenden technischen und organisatorischen Maßnahmen im Sinne des Art. 32 DSGVO getroffen, um Vertraulichkeit, Verschlüsselung und Pseudonymisierung, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit sowie entsprechende Prüfverfahren zu gewährleisten.

Inhaltsverzeichnis

1.0 Vertraulichkeit

1.1 Zugangskontrolle

Der Zugang von Unbefugten zu IT-System- und Verarbeitungseinrichtungen, mit denen die Verarbeitung durchgeführt wird, ist untersagt.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Login mit Benutzername und Passwort ☑ Automatische Desktopsperre ☑ Firewall/Virenschutz für Rechner/Geräte ☑ Login mit biometrischen Daten	☑ Verwalten von Benutzerberechtigungen ☑ Richtlinie “Clean desk” ☑ Richtlinie “Sicheres Passwort” ☑ Zentrale Passwortvergabe ☑ Anzahl der Systemadministratoren auf das Notwendigste begrenzt

1.1 Zugriffskontrolle

Es wird gewährleistet, dass die zur Nutzung eines automatisierten Verarbeitungssystems befugten Personen nur Zugang zu den personenbezogenen Daten erhalten, für die ihre Zugriffsberechtigung gilt.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Netzsicherheit ☑ Host-basiertes Intrusion Detection System (IDS) ☑ Kontrolle der Zugriffsberechtigung auf Kundensysteme durch Auftraggeber	☑ Vergabe von Zugriffsrechten ☑ Dokumentation der Ausgabe von Hardware an Mitarbeiter ☑ Rollen- und Berechtigungskonzept ☑ Standort des Servers in Raum ausgelagert ☑ Sicherung des Serverraums vor Zutritt unberechtigter Personen

	☑ Sicherung des Serverraums vor Zutritt unberechtigter Personen

1.3 Trennungskontrolle

Es wird sichergestellt, dass personenbezogene Daten, die für verschiedene Zwecke erhoben werden, getrennt verarbeitet werden können und von anderen Daten und Systemen so getrennt sind, dass eine ungeplante Nutzung dieser Daten für andere Zwecke ausgeschlossen ist.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Trennung von Entwicklungs-, Test- und Betriebsumgebungen (gem. 12.1.4 ISO/IEC 27001:2013) ☑ Softwareseitige Mandantentrennung ☑ Trennung von Netzwerken (gem. 13.1.3 ISO/IEC 27001:2013)	☑ Trennung von Daten, die verschiedene Kunden/Auftraggeber betreffen ☑ Trennung von Daten, die zu verschiedenen Zwecken verarbeitet werden

1.4 Verschlüsselung und Pseudonymisierung

Es wird sichergestellt, dass personenbezogene Daten im System nur in einer Weise gespeichert werden, die es Dritten nicht ermöglicht, die betroffenen Personen zu identifizieren.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Schlüsselverwaltung (gem. 10.1.2 ISO/IEC 27001:2013) ☑ Datenbank- und Speicherverschlüsselung ☑ Verschlüsselter Austausch von Informationen und Dateien	☑ Verschlüsselung von Speichergeräten auf Laptops

☑ Datenübertragung über verschlüsselte Datennetze oder Tunnelverbindungen („data in transit“) ☑ Pseudonymisierung personenbezogener Daten	

2.0 Integrität

2.1 Übermittlungskontrolle

Es wird sichergestellt, dass die Vertraulichkeit und Integrität privater Daten bei der Übertragung und beim Transport der Speichermedien geschützt sind.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Übermittlungsverschlüsselung („Data in Transit“) ☑ E-Mail-Verschlüsselung (SSL, TSL) ☑ Sichere Vernichtung nicht mehr benötigter Datenträger	☑ Verbot der Weitergabe an unbefugte Dritte ☑ Weitergabe in anonymisierter oder pseudonymisierter Form

2.2 Eingangskontrolle

Es soll sichergestellt werden, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welchem Zeitpunkt und von wem in automatisierte Verarbeitungssysteme eingegeben oder geändert worden sind.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Protokollierung der Systemaktivitäten im Admin- und Kundensystem sowie Auswertung ☑ Login- und Logout-Protokollierung ☑ Dokumentation von durchgeführten	

Wartungs-, Fernwartungs- oder Reparaturarbeiten am IT-System	

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Sicherstellen, dass personenbezogene Daten gegen versehentliche Zerstörung oder Verlust geschützt sind.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☑ Datensicherungsverfahren/Backups ☑ IT-Störungsmanagement (gem. 16 ISO/IEC 27001:2013) ☑ Georedundanz in Bezug auf die Serverinfrastruktur von Produktivdaten und Backups	☑ Unterbrechungsfreie Stromversorgung ☑ Warnsysteme zur Überwachung der Erreichbarkeit und des Zustands der Server-Systeme

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Beschreibung der Verfahren zur regelmäßigen Überprüfung, Bewertung und Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
	☑ Durchführung von internen Audits ☑ Konzept Durchführung von Risikobewertungen ☑ Verfahren zur kontinuierlichen Verbesserung des Datenschutz- und Informationssicherheitsmanagement systems ☑ Überprüfung der Einhaltung von Sicherheitsrichtlinien und Standards (gem. 18.2.2 ISO/IEC 27001:2013) ☑ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

4.2 Vertragsüberwachung

Es wird gewährleistet, dass private Daten, die im Auftrag des Kunden verarbeitet werden, nur gemäß den Anweisungen des Kunden verarbeitet werden können.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Technische Maßnahmen	Organisatorische Maßnahmen
	☑ Auftragsverarbeitung gem. Art. 28 DSGVO

	☑ Eindeutige Vertragsgestaltung, schriftliche Festlegung der Weisungen ☑ Durchführung regelmäßiger Kontrollen / Anforderung von Nachweis ☑ Sorgfältige Auswahl von Lieferanten ☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

5.0 Privacy by Default und Privacy by Design

5.1 Privacy by Default

Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Das heißt, bereits die Werkseinstellungen sollen datenschutzfreundlich ausgestaltet werden. Hierdurch sollen vor allem die Nutzer geschützt werden.

5.2 Privacy by Design

Privacy by Design bedeutet „Datenschutz durch Technikgestaltung“. Das heißt, dass bereits bei der Entwicklung oder dem Einkauf von Software auf eine datenschutzfreundliche Gestaltung geachtet werden soll.

Die avy health GmbH hat die Anforderungen folgendermaßen umgesetzt:

Privacy by Default	**Privacy by Design**
☑ Transparente Einstellungen und Optionen für den Nutzer zum Wählen der Einstellungen. ☑ Voreinstellungen, bei denen die Software nur die nötigsten Daten sammelt. ☑ Transparente Information der betroffenen Personen. ☑ Voreinstellungen, bei denen die Software die Zugänglichkeit von Daten auf das Nötigste beschränkt	☑ Bei der Entwicklung oder beim Kauf von Software wird darauf geachtet, dass die Software so wenige Daten wie möglich für die Verarbeitung anfordert/benötigt ☑ Möglichkeiten bei der Software mit pseudonymisierten oder anonymisierten Daten zu arbeiten

6.0 Zertifikate

6.1 Externes Datenschutz Audit

Ein Audit bezeichnet allgemein eine Prüfung, mit der man bestimmte Parameter erfasst, bewertet und daraus entsprechende Konsequenzen ableitet. Mit einem Datenschutzaudit werden die entsprechenden Bedingungen im Bereich Datenschutz festgestellt, bewertet und im Anschluss daraus ein entsprechendes Datenschutzkonzept entwickelt.
Die avy health GmbH hat im September 2022 ein Datenschutzaudit der PROLIANCE GmbH abgeschlossen.

Stand: November 2022