Technische und Organisatorische Maßnahmen- Übersicht

Personio 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.

1. Vertraulichkeit

1.1 Organisatorische Steuerung

Es soll sichergestellt werden, dass die interne Organisation die spezifischen Anforderungen des Datenschutzes erfüllt.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Organisatorische Anweisungen (gem. 5 und 6 ISO/IEC 27002/2017	X	Bestellung eines Datenschutzbeauftragten
X	Verpflichtung zur Vertraulichkeit und zum Datenschutz	X	Datenschutzschulungen
X	Einschränkungen der privaten und geschäftlichen Nutzung von Kommunikationsgeräten	X	Zuverlässigkeit des Personals (gem. 7 ISO/IEC 27002:2017)

1.2 Verschlüsselung und Pseudonymisierung von personenbezogenen Daten

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

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Schlüsselverwaltung (gem. 10.1.2 ISO/IEC 27002:2017)	X	Datenbank- und Speicherverschlüsselung
X	Datenübertragung über verschlüsselte Datennetze oder Tunnelverbindungen („data in transit“)	X	Verschlüsselung von mobilen Speichermedien

X	Verschlüsselung von Speichergeräten auf Laptops	X	Verschlüsselter Austausch von Informationen und Dateien
X	E-Mail-Verschlüsselung		

1.3 Physische Zugangskontrolle

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

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Elektronische Türschlösser	X	Kontrollierte und dokumentiere Schlüsselverteilung
X	Beaufsichtigung und Begleitung von Fremden	X	Absicherung von Räumen mit erhöhtem Schutzbedürfnis
X	Geschlossene Türen und Fenster	X	Physische und umgebungsbedingte Sicherheit von Serversystem in Rechenzentren
X	Einsatz von Wachpersonal	X	Sonstige: Verwendung von Mitarbeiterausweisen zur Identifizierung berechtigter Personen und zum Öffnen verschlossener Türen Videoüberwachung in sensiblen Bereichen (Rechenzentrum)

1.4 Berechtigungskontrolle

Die Nutzung und Verarbeitung datenschutzrechtlich geschützter Daten durch Unbefugte wird verhindert.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Verwendung von Authentifizerungsverfahren	X	Berechtigungsbestimmung- und vergabe nach Freigabe durch die Administration
X	Verwendung sicherer Passwörter	X	Verbot der Weitergabe von Passwörtern und Nutzung von „Shared Accounts“
X	Automatische Sperrung bei Inaktivität	X	Einsatz von Anti-Viren-Software
X	Clean Desk Policy	X	VPN-Verbindung zu öffentlichen Drahtlosnetzwerken und Verbindung zum Firmennetz

1.5 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.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Rollen- und Berechtigungskonzept	X	Kontrolle der Zugriffsberechtigung auf Kundensysteme durch Auftraggeber
X	Vergabe von Zugriffsrechten	X	Host-basiertes Intrusion Detection System (IDS)
X	Netzsicherheit	X	Protokollierung von An- und Abmeldevorgängen

1.6 Trennbarkeit

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.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Trennung von Entwicklungs-, Test- und Betriebsumgebungen (gem. 12.1.4 ISO/IEC 27002:2017)	X	Trennung von Netzwerken (gem. 13.1.3 ISO/IEC 27002:2017)
X	Softwareseitige Mandantentrennung		

2. Integrität

2.1 Übermittlungskontrolle

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

Personio hat die Anforderungen in folgender Art umgesetzt:

X	Übermittlungsverschlüsselung („Data in Transit“)	X	Verbot der Weitergabe an unbefugte Dritte

2.2 Eingabekontrolle

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.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Protokollierung der Systemaktivitäten im Admin- und Kundensystem sowie Auswertung		

3. Verfügbarkeit

3.1 Verfügbarkeitskontrolle

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

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Datensicherungsverfahren/Backups	X	Georedundanz in Bezug auf die Serverinfrastruktur von Produktivdaten und Backups
X	Kapazitätsmanagement	X	Warnsysteme zur Überwachung der Erreichbarkeit und des Zustands der Server-Systeme
X	IT-Störungsmanagement (gem. 16 ISO/IEC 27002:2017)	X	Brandmelde- und Brandbekämpfungssystem
X	Unterbrechungsfreie Stromversorgung		

3.2 Wiederherstellbarkeit

Es wird sichergestellt, dass Systeme im Falle eines physischen oder technischen Ausfalls zuverlässig wiederhergestellt werden können.

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Notfallplan („Disaster Recovery Concept“)

4. Überprüfung und Evaluierung

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

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Einrichtung Team Datenschutz und Informationssicherheit	X	Risikomanagement
X	Unabhängige Überprüfung der Informationssicherheit (gem. 18.2.1 ISO/IEC 27002:2017)	X	Durchführung von internen Audits
X	Überprüfung der Einhaltung von Sicherheitsrichtlinien und Standards (gem. 18.2.2 ISO/IEC 27002:2017)	X	Überprüfung der Einhaltung technischer Spezifikationen (gem. 18.2.3 ISO/IEC 27002:2017)
X	Verfahren zur kontinuierlichen Verbesserung des Datenschutz- und Informationssicherheitsmanagementsystems		

4.1 Vertragsüberwachung

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

Personio hat die Anforderungen folgendermaßen umgesetzt:

X	Auftragsverarbeitung gem. Art. 28 DSGVO	X	Sorgfältige Auswahl von Lieferanten

X	Durchführung regelmäßiger Kontrollen / Anforderung von Nachweisen	