Ostendis E-Recruiting-System

Technische & organisatorische Massnahmen Ostendis AG

Version: 08.08.2023

Dieses Dokument legt die technischen und organisatorischen Massnahmen («TOM») der Ostendis AG dar von:

Ostendis AG
Seetalstrasse 35
5706 Boniswil AG
Schweiz

PRÄAMBEL

(A) Mittels diesen «TOM» möchten die Ostendis AG über die getroffenen technischen und organisatorischen Massnahmen informieren, die im Zusammenhang mit der Verarbeitung und Speicherung von personenbezogenen Daten stehen.

(B) Diese «TOM» sind darauf ausgelegt, den folgenden gesetzlichen Bestimmungen nachzukommen:
   a. Schweizer Datenschutzgesetz (01.09.2023, Art. 8 nDSG, ab 01.09.2023)
   b. Europäische Datenschutz Grundverordnung (Art. 24, 32 Abs. 1 EU-DSGVO ab 25.05.2018)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Massnahmen Büroräumlichkeiten:

- Türen mit Sicherheitsschliesssystemen
- Besucherregelung
- Besucherbegleitung durch Mitarbeitende
- Vertragliche Absicherung Servicepersonal (Reinigung)

Massnahmen Rechenzentren:

- Videoüberwachung
- Automatisches Zugangskontrollsystem
- Elektronisches Schliesssystem mit Berechtigungsmanagement
- Restriktive Zugangsrichtlinien
- Wachpersonal
- Besucherbegleitung ausschliesslich durch berechtigte Mitarbeitende
- Vertragliche Absicherung mit Dienstleistern (Wartung)
- Sicherheitsschlösser

1.2 Zugangskontrolle

Massnahmen:

- strikte Fernzugriffsrichtlinien
- wo möglich Zwei-Faktor-Authentifizierung
- Firewall
- regelmässige Überprüfung von Berechtigungen
- verpflichtende Verschlüsselung von Datenverbindungen
- Verhaltensrichtlinien für Mitarbeitende im Umgang mit schützenswerten Daten
- Passwortrichtlinien
- Zentrales Passwortmanagement
- restriktive Berechtigungsregelung für besonders schützenswerte Daten
- Mobile und Telearbeit Policy

1.3 Zugriffskontrolle

Massnahmen:

- Professionelle Vernichtung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verhaltensrichtlinien Administratoren
- Verwaltung Benutzerrichtlinien durch Administratoren
- Vergabe von Rechten nach dem «Least Privilege» Prinzip

1.4 Trennungskontrolle

Massnahmen:

- Trennung von Produktiv-, Qualitätssicherungs- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- restriktives Berechtigungskonzept

1.5 Anonymisierung /Pseudonymisierung

Massnahmen:

- Anonymisierung der Daten für statistische Auswertungen
- Keine Pseudonymisierung personenbezogenen Daten

2. Integrität

2.1 Weitergabekontrolle

Massnahmen:

- Einsatz VPN
- Protokollierung der Zugriffe und Abrufe
- Verschlüsselte Übertragung von Daten
- Weitergabe in anonymisierter oder pseudonymisierter Form

2.2 Eingangskontrolle

Massnahmen:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit

1. 3.1 Verfügbarkeitskontrolle

Massnahmen:

- Feuer- und Rauchmeldeanlage
- Automatisches Feuerlöschsystem
- Klimaüberwachung Serverräume
- USV
- Notstromgenerator
- Redundante Stromversorgung
- RAID Systeme
- Videoüberwachung
- Alarmanlage
- Backup- und Recoverykonzept (Business Continuity Policy)
- Monitoringsysteme
- Offsite Backups
- Existenz eines Notfallplans
- Redundante Netzzuleitung
- Regelmässige Überprüfung und Tests der Notfallpläne
- Incident-Management-Policy

4. Verfahren für regelmässige Überprüfung, Bewertung und Evaluierung

4.1 Datenschutzmassnahmen

Massnahmen:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- regelmässige Überprüfung der Wirksamkeit der technischen Schutzmassnahmen
- Interner Datenschutzbeauftragte
- Datenschutzpolicy für Mitarbeitende und Awarenesstraining
- Schulung und Sensibilisierung der Mitarbeitenden
- Interner Informationssicherheitsbeauftrage
- Externe Audits
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Incident-Response-Managment

Massnahmen:

- Einsatz von Firewall
- regelmässige Aktualisierung
- regelmässige Überprüfung nach Sicherheitslücken
- Risikomanagement
- Spamfilter
- Virenscanner
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Incident-Management-Policy

4.3 Datenschutzfreundliche Voreinstellungen

Massnahmen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.4 Auftragskontrolle

Massnahmen:

- Keine Subunternehmer für Auftragsverarbeitung
  Hiermit versichern wir, aktuell keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen

Dokumentgültigkeit

Diese «TOM» treten im Einklang mit dem neuen CH-DSG per 01.09.2023 in Kraft.

Diese «TOM» sind nach dem gesetzlich angedachten Prinzip der Verhältnismässigkeit erstellt.

Diese «TOM» werden quartalsweise durch das Datenschutzteam überprüft.

Die Ostendis AG behält sich das Recht vor, dieser «TOM» jederzeit zu ändern, damit wir diese laufenden Veränderungen, neuen Gegebenheiten und unserem Wachstum stetig anpassen können. Diese Änderungen sind grundsätzlich nur additiver Natur. Werden Massnahmen ersatzlos gestrichen, so werden diese Änderungen proaktiv kommuniziert und bedingen den Abschluss einer Einverständniserklärung seitens der Kundinnen der Ostendis AG. Diese Einverständniserklärung kann auch elektronisch erfolgen.

Sollen Teile dieser «TOM» rechtswidrig, unwirksam, ungültig oder undurchführbar sein, so bleiben die restlichen Bestimmungen in ihrer Wirksamkeit und Gültigkeit unberührt.

Verantwortlich für diese TOM

Da wir dem Datenschutz in unserem Unternehmen einen sehr hohen Stellenwert beimessen, haben wir ein internes Datenschutzteam aufgebaut, damit wir unserer Auskunftspflicht bei allen Anfragen zeitnah nachkommen können.

Weitere Informationen und die Ansprechpartner des Datenschutzteams finden Sie im Dokument «Datenschutzerklärung_Ostendis_AG»

Verantwortlich für dieses Dokument:

Boniswil, 08.08.2023

Ostendis AG

Philippe Moser, CEO