TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Beschreibung der technischen und organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO

Version 4.1 / Gültig ab 06.04.2022

DE COOR GmbH | Altlaufstraße 38/40 | 85635 Höhenkirchen-Siegertsbrunn | T 08102 8979616 | HRB 194229

AT COOR GmbH | Schillerstraße 27 | 5020 Salzburg | T 0662 452277 | FN 138102t

TECHNISCHE
UND ORGANISATORISCHE MASSNAHMEN

Beschreibung der technischen und organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO.

Wir sehen die Wahrung von Datenschutzrechten als Teil unserer sozialen Verantwortung. 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 wir geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. VERTRAULICHKEIT

Wir befinden uns in einem besonderen Vertrauensverhältnis zu unseren Kunden. Wir gehen daher mit allen erlangten Daten sowie Informationen verantwortungsbewusst um und wahren die Verschwiegenheit.

1.1. Zutrittskontrolle

Verwaltung:

- Alarmanlage
- Schlüsselregelung (Schlüsselausgabe etc.)
- Verschlossene Türen bei Abwesenheit
- Besucherregistrierung

Rechenzentrum (COOR SaaS, COOR SaaS Enterprise, COOR-ITSC):

- Zutrittskontrolle gemäß ISO/IEC 27001 A.11
- Videoüberwachung mit Archivierung
- 24/7 Sicherheitsdienst vor Ort
- Biometrische Zutrittskontrolle mit 24/7-Zutritt über Transponderkarte
- Raum-in-Raum-Konzept trennt IT-Flächen von Außenwänden
- Perimeterschutz mit Sicherheitszaun und Vereinzelungsschleusen

1.2. Zugangskontrolle

Die folgenden Maßnahmen verhindern, dass COOR Server von Unbefugten genutzt werden können:

- Verwendung von Benutzerrollen, Benutzerrechten
- Authentifikation mit Benutzername und Passwort
- Computer / Laptop Inhalte von COOR Mitarbeitern sind verschlüsselt
- Verwendung von Passwort-Manager Software bei COOR
- Verwendung einer Software Firewall auf COOR Servern
- Richtlinien für Passwörter/Löschen/Clean-Desk

Rechenzentrum (COOR SaaS, COOR SaaS Enterprise, COOR-ITSC):

- Videoüberwachung mit Archivierung
- 24/7 Sicherheitsdienst vor Ort
- Biometrische Zutrittskontrolle mit 24/7-Zutritt über Transponderkarte
- Raum-in-Raum-Konzept trennt IT-Flächen von Außenwänden
- Perimeterschutz mit Sicherheitszaun und Vereinzelungsschleusen
- Rack-Überwachung mit leistungsfähigen Monitoring-Systemen

1.3. Zugriffskontrolle

Folgende Maßnahmen gewährleisten, dass COOR Mitarbeiter ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Administrationszugriff ist auf die notwendigsten Mitarbeiter beschränkt.
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Verschlüsselung von Datenträgern, sofern ein entsprechender Schutzbedarf gegeben ist
- Einsatz von Aktenvernichtern

Rechenzentrum (COOR SaaS, COOR SaaS Enterprise, COOR-ITSC):

- Zugriffskontrolle gemäß ISO/IEC 27001 A.9

2. INTEGRITÄT

2.1. Weitergabekontrolle / Übermittlungskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Daten wie Sicherungen werden rein auf elektronischen Transportwegen übertragen.
- Die Übertragung läuft ausschließlich über verschlüsselte Kanäle.

2.2. Eingabekontrolle

Maßnahmen zur Prüfung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen

2.3. Auftragskontrolle (Noris Network AG)

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Sorgfältige Auswahl des Auftragnehmers hinsichtlich Datensicherheit
- Protokollierung aller eingegeben Daten
- Schriftliche Weisungen an den Auftragnehmer gemäß AVV

3. VERFÜGBARKEITSKONTROLLE

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Automatische tägliche Datensicherung
- Regelmäßige Tests der Datensicherung und Datenwiederherstellung
- Datensicherungen werden an einem sicheren, (ggfs. ausgelagerten) Ort aufbewahrt.
- Backup und Wiederherstellungskonzept für alle Daten
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage im Rechenzentrum

4. TRENNUNGSGEBOT

Folgende Maßnahmen werden zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von personenbezogenen Daten mit unterschiedlichen Zwecken getroffen:

- Berechtigungskonzept und Datenbankberechtigungen
- Softwareseitige Mandantentrennung
- Trennung von Produktiv und Testsystem

5. DATENSCHUTZMANAGEMENT

Die innerbetriebliche Organisation ist durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Nachweise über durchgeführte Schulungen der Mitarbeiter zum Datenschutz liegen vor
- Nachweise über Einhaltung der datenschutzrechtlichen Verpflichtungen der verarbeitenden Mitarbeiter liegen vor

- Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (in Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Datenschutzbeauftragter ist schriftlich bestellt
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt

6. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
- COOR Datenschutz-Managementsystem (DSMS) ist vorhanden