Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Conundra BV

Sicherheitskonzept 3
Grundsätzliche Maßnahmen 3
Zutrittskontrolle 3
Zugangskontrolle / Zugriffskontrolle 4
Weitergabekontrolle 4
Eingabekontrolle 4
Auftragskontrolle 4
Verfügbarkeitskontrolle / Integrität 5
Gewährleistung des Zweckbindungs-/Trennungsgebotes 5

Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- There is an internal data protection management system, compliance with which is constantly monitored and evaluated as required and at least annually.
  We have an annual pen test, annual internal audit review and annual external audit review.

- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
  We have an onboarding/offboarding process.
  User access matrix is also reviewed regularly.

- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.
- Clean-Desk-Politik, damit unbegleitete externe Dienstleister keinen Zugang zu personenbezogenen Daten haben.

Zutrittskontrolle

- Sicherheitsschlösser
- Die Haustür ist mit Schlüssel und Sicherheitscode verschlossen.
- Zutrittsregelungen für betriebsfremde Personen
  Es gibt eine Politik für unbegleitete Dienstleistungsanbieter.

- Anweisung zur Fenstersicherung
  Die Fenster sind von der letzten Person, die das Gebäude verlässt, zu verschließen.

- Beaufsichtigung von Hilfskräften
  Alle externen Besucher werden begleitet.
  Wenn sie nicht begleitet werden (z. B. Reinigungspersonal), unterzeichnen sie ein spezielles Dokument (DOC-024).

Zugangskontrolle / Zugriffskontrolle

- Einsatz von VPN-Technologie
- Verschlüsselung von mobilen Geräten (Laptops)
- Mindestpasswortlängen und Passwortmanager
- Berechtigungs-/ Authentifizierungskonzepte mit auf das Nötigste beschränkten Zugriffsregulierungen
- Stets aktuelle Softwareversionen
- Stets aktueller Virenschutz
- Einsatz von Intrusion-Detection-Systemen
  Microsoft defender.

- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
- Protokollierung von Zugriffen auf Daten
- Richtlinie zum Einsatz von USB-Sticks
  Wir haben eine Richtlinie, die besagt, dass wir keine USB-Sticks verwenden dürfen.

- Verschlüsselung von Festplatten (FileVault, Bitlocker)
- Ordnungsgemäße Vernichtung von Datenträgern
  Es gibt ein Verfahren zum Löschen von Laptops.

Weitergabekontrolle

- Verschlüsselung von Datenträgern und Verbindungen
- Festlegung und Dokumentation der Empfänger
  Wir haben ein Verfahren zur Datenklassifizierung.

Eingabekontrolle

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
  Wir haben eine Zugangskontrollpolitik.

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
  Begrenzt auf OptiFlow-Downloads.

Auftragskontrolle

- Kontrolle der Einhaltung bei Auftragnehmern
  Die Anforderungen sind im Vertrag und in der Vertraulichkeitsvereinbarung festgelegt.

- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  Entweder wird der PC angemeldet und verwaltet, das An- und Abmelden wird kontrolliert.
  Oder sie haben Zugriff auf die Webversion, der widerrufen werden kann.

Verfügbarkeitskontrolle / Integrität

- Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
- Ständig kontrolliertes Backup- und Recoverykonzept
- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
- Durchführung von Belastbarkeitstests

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Logische Mandantentrennung (Software)
- Trennung von Produktiv- und Testsystem