TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN
gem. Art. 32 DSGVO

(Stand: 15. September 2023)

Straide GmbH trifft geeignete technische und organisatorische Maßnahmen, um ein angemessenes Schutzniveau im Rahmen des Datenschutzes und der Datensicherheit für die eigenen Produkte und Datenverarbeitungstätigkeiten zu gewährleisten. Straide GmbH stellt selbst oder mittels dritter Dienstleister insbesondere die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der eingesetzten Systeme bzw. Anwendungen sicher und hat hierzu die folgenden Maßnahmen implementiert. Die Maßnahmen werden durch die Geschäftsleitung laufend kontrolliert und ggf. angepasst.

I. GEWÄHRLEISTUNG DER VERTRAULICHKEIT

ZUTRITTSKONTROLLE

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Dokumenten und Datenträger physisch verwehren:

- Die Betriebsräume sind nur durch Passieren des immer besetzten Empfangsschalters zu betreten.
- Betriebsfremde Personen (z.B. Besucherinnen und Besucher) werden durch die Geschäftsleitung identifiziert und werden ausschließlich in Begleitung durch den Betrieb geführt und es wird ein Besucherbuch / Protokoll der Besucher geführt.
- Der Zutritt zu den Betriebsräumen wird durch ein manuelles Schließsystem geschützt.
- Die Schlüsselvergabe an Mitarbeiter wird dokumentiert.
- Es erfolgt eine sorgfältige Auswahl von Reinigungspersonal und diese sind an Vertraulichkeitsvereinbarungen gebunden.

ZUGANGSKONTROLLE

Maßnahmen, die verhindern, dass Unbefugte personenbezogene Daten verarbeiten oder nutzen können:

- Verschlüsselung von Daten im Ruhezustand und während der Übermittlung.
- Authentifizierung mittels Benutzername und Passwort.
- Verwaltung von Benutzerberechtigungen und Erstellen von Benutzerprofilen.
- Passwörter müssen vordefinierte Richtlinien erfüllen.
- Der Login wird bei Unregelmäßigkeiten durch das System gesperrt.
- Einsatz von Anti-Viren-Software, Firewall-Systemen (Hardware/Software) und Intrusion-Detection-Systemen.
- Die Verwaltung der Sicherheitssoftware wird regelmäßig sichergestellt und erfolgt nur durch die Geschäftsleitung.
- Remote-Zugriffe auf die Datenverarbeitungssysteme erfolgen stets über eine gesicherte und verschlüsselte IPSEC VPN-Verbindung.

ZUGRIFFSKONTROLLE

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen

Straide GmbH GmbH
Alser Straße 27/1/6
1080 Wien (in den Räumlichkeiten der Sportordination)

Tel: +43 1 2280028
Email: office@straide.com
Firmenbuchnummer: FN 540426 w
UID Nummer: ATU 76067809

können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einsatz von Berechtigungskonzepten.
- Minimale Anzahl von Administratoren.
- Verwaltung der Benutzungsrechte durch Administratoren.
- Protokollierung von Zugriffen auf Anwendungen (konkret bei Eingabe, Änderung und Löschung von Daten).
- Vorgaben zu Passwörtern (Passwortlänge und Passwortwechsel).
- Regelmäßige Sicherheitsupdates.

TRENNUNGSKONTROLLE

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, sodass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:

- Physikalische Trennung (Systeme / Datenbanken / Datenträger).
- Logische Kunden-/Mandantentrennung.
- Trennung von Produktiv- und Testumgebung.
- Physikalische und/oder logische Trennung von Produktivumgebung zu Datensicherung.
- Steuerung über Berechtigungskonzept.

II. GEWÄHRLEISTUNG DER INTEGRITÄT

WEITERGABE- UND ÜBERTRAGUNGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, mit denen überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist:

- Bereitstellung über verschlüsselte Verbindungen.
- Protokollierung der Zugriffe und Abrufe von Dokumenten und personenbezogenen Daten.

EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- 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.

III. GEWÄHRLEISTUNG DER VERFÜGBARKEIT

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Von den Instanzen und den dazugehörigen Datenbanken werden in regelmäßigen Abständen in demselben Rechenzentrum, als auch zusätzlich an einem vom Rechenzentrum ausgelagerten Ort Sicherheitskopien angefertigt, die bei Bedarf zurückgespielt werden können.
- Verwendung der von unseren Dienstleistern angebotenen Technologien wie DDoS-Schutz.

- Einsatz einer unterbrechungsfreien Stromversorgung.
- Spiegelung der Festplatten bei allen relevanten Servern und regelmäßige Backups der Daten und virtuellen Maschinen.
- Überwachung aller internen Systeme und automatisierte Durchführung diverser Status-Prüfungen in der Nacht.
- Backup- und Wiederanlaufkonzept, welches sicherstellt, dass eine System- und Datenwiederherstellung schnellstmöglich durchgeführt werden kann.
- Vorab definierte Eskalationskette, die vorgibt, wer im Fehlerfall zu informieren ist, um die betroffenen Systeme schnellstmöglich wiederherzustellen.