Kordiam GDPR Dokumentation -
Technische und organisatorische Maßnahmen (TOMs)

Anlage 3 zur Kordiam Auftragsdatenvereinbarung (AVV)

Einleitende Bemerkungen

Die nachfolgend genannten Maßnahmen beziehen sich auf Aufgaben, die von der Kordiam GmbH wahrgenommen werden. Dabei handelt es sich um Aufgaben der Anwenderbetreuung und der Produktentwicklung.

Der Betrieb, die Wartung, die Entwicklung und das Testen der Kordiam Anwendung werden von Partnerunternehmen durchgeführt, mit denen entsprechende Vereinbarungen getroffen wurden.

Weitere Informationen zu diesen Partnern finden Sie über https://kordiam.io/de/rechtliche-themen.

Die Struktur des nachfolgenden Inhalts ergibt sich aus Art. 32 (1) GDPR.

Anonymisierung und Verschlüsselung

- Verschlüsselte Datenübertragung zwischen Client und Server (SSL, RSA 2048 Bit)
- Verschlüsselung der Daten at Rest
- Anonymisierung von personenbezogenen Daten für Entwicklungs- und damit verbundene Testzwecke

Vertraulichkeit

- Strenges Bürozugangskonzept mit mehreren verschlossenen Türen, deren Schlüssel nur an reguläre Mitarbeiter und Reinigungspersonal ausgegeben werden.
- Zugang zum Büro für Besucher nur in Begleitung eines Mitarbeiters
- Verriegelungskonzept für Fenster
- Dokumentiertes Systemzugangskonzept einschließlich der Entfernung von Benutzerzugängen mit regelmäßigen Überprüfungen
- Einsatz von Antivirensoftware einschließlich automatischer Updates
- Automatisch aktivierte und passwortgeschützte Computersperre
- Sichere und regelmäßig aktualisierte relevanter Passwörter mit einem sehr begrenzten Kreis von Mitarbeitern, die diese erhalten
- Zwei verschiedene Anmeldedaten für den Zugriff auf Kundendaten erforderlich
- Kein Zugang zu persönlichen Daten ohne Authentifizierung
- Verhinderung von Brute-Force-Passwort-Eingabeversuchen bei Kordiam
- Einschränkung des Zugangs zu Kordiam nur aus dem Firmennetzwerk des Kunden möglich (aufpreispflichtig)
- Standard- und erweiterte Passwortanforderungen verfügbar
- Protokollierung von Zugriffen auf die Anwendung (einschließlich fehlgeschlagener Zugriffe)

- Detaillierter Prozess mit den Kunden, der sicherstellt, dass Daten nur auf der Grundlage individueller schriftlicher Anfragen von berechtigten Personen auf Kundenseite bearbeitet werden
- Anonymisierung von Daten für Entwicklungs- und Testzwecke
- Keine Nutzung von mobilen Datenträgern

Integrität

- Detaillierte Nachverfolgung von Eingaben, Bearbeitungen und Löschungen
- Regelmäßige Datensicherungen zur Sicherstellung der Verfügbarkeit einer unverfälschten Datenbankversion
- Logische Mandantentrennung in der Anwendung
- Trennung von Produktions-, Test- und Entwicklungssystemen
- Regelmäßige Updates und Patches von externen Softwarekomponenten

Verfügbarkeit und Ausfallsicherheit

- Dokumentierte Prozesse zur Reaktion auf Vorfälle
- Hochverfügbares Domain-Hosting
- Redundante Datenbanken
- Mehrere Datensicherungen pro Tag
- Sicherung der kurzfristigen Planungsdaten im xls-Format auf dem ftp-Server des Kunden (aufpreispflichtig)
- Verfahren zur Löschung (Löschkonzept)
    - Der Auftraggeber ist für die Löschung der einzelnen Nutzerprofile und der damit verbundenen Daten während der Laufzeit des Kordiam Vertrages verantwortlich.
    - Der Datenverarbeiter löscht die Nutzerprofile des Verantwortlichen innerhalb von 90 Tagen nach Beendigung des Vertrages.
    - Backups, die möglicherweise personenbezogene Daten enthalten, die aus dem Produktivsystem gelöscht wurden, werden maximal sechs Monate aufbewahrt.

Fähigkeit zur Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten

- Dokumentierte und regelmäßig getestete Failover-Verfahren
- Automatisierung von Prozessen zur Wiederherstellung der Anwendung oder von Teilen der Anwendung

Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- Regelmäßige Überprüfung der Datenschutzmaßnahmen
- Regelmäßige Schulung der Mitarbeiter zu Datenschutzmaßnahmen
- Regelmäßige Überwachung von Partnerunternehmen hinsichtlich der Datenschutzmaßnahmen