lexiCan®
Business

Technische und organisatorische Maßnahmen (TOM)

Stand: November 2023

1. Einleitung

In Übereinstimmung mit den Datenschutzbestimmungen und -anforderungen setzen wir in der vetafab Software GmbH eine Reihe von technischen und organisatorischen Maßnahmen (TOM) um, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu gewährleisten. Dieses Dokument beschreibt maßgebliche TOM in Übereinstimmung mit den geltenden Datenschutzgesetzen.
Wir prüfen in regelmäßigen Abständen und anlassbezogen die Effektivität und Angemessenheit dieser Maßnahmen und setzen auf dieser Grundlagen Optimierungen um.

2. Verantwortlicher Datenschutzbeauftragter

Günther Eufinger
eufinger@lexican.de

vetafab Software GmbH
Konrad-Adenauer-Str. 32

D-64401 Groß-Bieberau

3. Zutrittskontrolle

a) Nur Betriebsangehörige haben Zutritt zu unseren Räumlichkeiten.

b) Besucher erhalten keinen Zutritt zu Räumlichkeiten in denen personenbezogene oder anderweitig sensible Daten verfügbar oder abrufbar sind.

4. Zugangskontrolle

a) Einrichtung von Zugriffsrechten: Nur autorisierte Mitarbeiter haben Zugriff auf Systeme, über die personenbezogene Daten abrufbar sind.

b) Es werden ausschließlich individuelle, persönliche Benutzerkennungen angewendet und keine Gruppenpasswörter genutzt.

c) Passwortschutz: Alle Benutzerkonten erfordern sichere, regelmäßig zu ändernde Passwörter.

d) Es besteht ein Berechtigungskonzept in dem Lese-, Schreib und Löschrechte festgelegt und Benutzerkonten zugeordnet sind

e) Überwachung des Datenzugriffs: Zugriffe auf personenbezogene Daten werden protokolliert und überwacht.

f) Es erfolgt eine systemseitige Bildschirmsperre bei Pausen mit Passwort-Aktivierung.

5. Eingabekontrolle

a) Über die systemseitige Protokollierung ist sichergestellt, dass nachvollzogen werden kann, wer wann was in die Datenverarbeitungssysteme eingegeben hat.

b) Die entsprechenden Protokolle werden für einen festgelegten Zeitraum aufbewahrt.

6. Vertraulichkeit

a) Verschlüsselung: Sensible Daten werden ausschließlich verschlüsselt übertragen.

b) Datensicherung: Regelmäßige Backups gewährleisten die Wiederherstellbarkeit von Daten bei Verlust oder Beschädigung.

c) Schutz vor Malware: Aktuelle Antivirensoftware und Firewalls sind installiert und werden regelmäßig aktualisiert.

d) Sicherer Datenverkehr: Der Datenaustausch erfolgt über sichere Kommunikationskanäle.

7. Datenschutz durch Technikgestaltung

a) Pseudonymisierung und Anonymisierung: Wenn möglich, werden Daten so verarbeitet, dass sie nicht mehr einer bestimmten Person zugeordnet werden können.

b) Privacy by Design: Datenschutzaspekte werden bereits in die Entwicklung neuer Systeme und Prozesse integriert.

8. Training und weitere Vorsorge

a) Datenschutzrichtlinien und Schulungen: Mitarbeiter werden über Datenschutzrichtlinien informiert und erhalten Schulungen.

b) Datenschutz-Folgenabschätzung (DSFA): Bei riskanten Datenverarbeitungstätigkeiten wird eine DSFA durchgeführt.

c) Notfallplanung: Ein Notfallplan zur Wiederherstellung von Daten und Diensten im Notfall ist vorhanden.

9. Überwachung und Audit

a) Regelmäßige Datenschutzüberprüfungen: Die TOM werden in regelmäßigen Abständen überprüft und aktualisiert.

b) Dokumentation und Protokollierung: Alle datenschutzrelevanten Aktivitäten werden dokumentiert.