

# Technisch-organisatorische Maßnahmen (TOM)

Stand: 11.04.2026

## Inhaltsverzeichnis

|                                                |   |
|------------------------------------------------|---|
| Präambel.....                                  | 2 |
| 1. Zutrittskontrolle (physischer Zugang).....  | 3 |
| 2. Zugangskontrolle (Systemzugang).....        | 3 |
| 3. Zugriffskontrolle (Berechtigungen).....     | 3 |
| 4. Weitergabekontrolle (Datenübertragung)..... | 3 |
| 5. Eingabekontrolle (Nachvollziehbarkeit)..... | 4 |
| 6. Auftragskontrolle.....                      | 4 |
| 7. Verfügbarkeitskontrolle.....                | 4 |
| 8. Trennungsgebot.....                         | 5 |
| 9. Ergänzende organisatorische Maßnahmen.....  | 5 |
| 10. Löschung und Datenminimierung.....         | 5 |
| 11. Subunternehmer.....                        | 6 |

## Präambel

Diese Darstellung der technisch-organisatorischen Maßnahmen (TOM) beschreibt die Maßnahmen, die die Polbeo Florian Dieckmann und Fabian Huschka GbR, Bärengasse 16, 67547 Worms (nachfolgend „Polbeo“ genannt) zum Schutz personenbezogener Daten im Rahmen seiner Tätigkeit umsetzt.

Die Maßnahmen dienen der Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten. Sie orientieren sich an den Anforderungen des Art. 32 DSGVO und berücksichtigen insbesondere den Stand der Technik, die Art, den Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Polbeo nutzt für die Bereitstellung seiner Leistungen überwiegend die Infrastruktur spezialisierter externer Dienstleister, insbesondere im Bereich Hosting und Systembetrieb. Die Verantwortung für die physische Sicherheit dieser Systeme liegt bei den jeweiligen Anbietern. Polbeo stellt sicher, dass die Nutzung dieser Infrastruktur unter Beachtung datenschutzrechtlicher Anforderungen erfolgt.

Die nachfolgend beschriebenen Maßnahmen bilden die tatsächlich umgesetzten technischen und organisatorischen Vorkehrungen ab. Sie werden regelmäßig überprüft und bei Bedarf angepasst, insbesondere bei Änderungen der eingesetzten Systeme oder organisatorischen Abläufe.

# **1. Zutrittskontrolle (physischer Zugang)**

- Zugriff auf Endgeräte nur durch autorisierte Personen
- Nutzung der Endgeräte ausschließlich durch Mitarbeitende
- Kein Zugriff durch Dritte (z. B. im Homeoffice-Umfeld)
- Physische Sicherheit der Serverinfrastruktur durch eingesetzte Hosting-Anbieter (insbesondere Uberspace)

# **2. Zugangskontrolle (Systemzugang)**

- Passwortschutz auf allen Systemen und Anwendungen
- Vollständige Festplattenverschlüsselung auf Notebooks
- Automatische Bildschirmsperre nach definierter Inaktivität
- Einsatz von Zwei-Faktor-Authentifizierung (2FA), vorzugsweise TOTP
- Zentrale Verwaltung von Zugangsdaten über Bitwarden
- Absicherung von Smartphones mittels PIN und/oder biometrischer Verfahren

# **3. Zugriffskontrolle (Berechtigungen)**

- Derzeit eingeschränkte Rollentrennung aufgrund der Unternehmensgröße
- Umfassende Zugriffsrechte der Geschäftsführung
- Zugriff für Mitarbeitende nach Aufgaben (Need-to-know-Prinzip)
- Zugriff auf interne Systeme (z. B. SuiteCRM) nur für zuständige Personen
- Zugriff auf Kundeninstanzen im Rahmen von Wartungs- und Supportleistungen

# **4. Weitergabekontrolle (Datenübertragung)**

- Ausschließlich verschlüsselte Datenübertragung:
  - HTTPS für Webanwendungen
  - SSH für Systemzugriffe

- E-Mail-Kommunikation über gesicherte IMAP-Verbindungen
- Einsatz von PGP-Verschlüsselung, soweit möglich
- Interne Kommunikation über eigenen Matrix-Server

## **5. Eingabekontrolle (Nachvollziehbarkeit)**

- Protokollierung von Zugriffen und Änderungen durch eingesetzte Systeme (z. B. Server-Logs, Anwendungsprotokolle)
- Keine zusätzliche manuelle Protokollierung durch Polbeo

## **6. Auftragskontrolle**

- Verarbeitung personenbezogener Daten ausschließlich im Rahmen vertraglicher Vereinbarungen
- Einsatz von Subunternehmern nur nach vertraglicher Einbindung
- Beachtung datenschutzrechtlicher Anforderungen bei allen Verarbeitungsvorgängen

## **7. Verfügbarkeitskontrolle**

- Automatisierte Erstellung verschlüsselter Backups
- Aufbewahrungsdauer der Backups: 7 Tage
- Speicherung der Backups derzeit innerhalb der Infrastruktur des Hosting-Anbieters
- Geplante Erweiterung um einen zusätzlichen, unabhängigen Backup-Speicherort
- Wiederherstellung von Systemen durch Einspielen von Sicherungskopien
- Wiederherstellungszeit in der Regel innerhalb eines Werktages, sofern keine außergewöhnlichen Umstände entgegenstehen
- Maßnahmen bei Datenverlust:
  - unverzügliche Information des betroffenen Kunden
  - Unterbindung weiterer Datenverluste

- ggf. Sperrung betroffener Systeme
- Analyse des Vorfalls und Ableitung von Präventionsmaßnahmen

## 8. Trennungsgebot

- Logische Trennung von Kundendaten durch separate Instanzen der bereitgestellten Systeme
- Zugriff auf Daten ausschließlich im Rahmen der jeweiligen Zweckbindung

## 9. Ergänzende organisatorische Maßnahmen

- Regelmäßige Schulung der Mitarbeitenden zu Datenschutz und Datensicherheit
- Vertragliche Verpflichtung zur Vertraulichkeit und Einhaltung datenschutzrechtlicher Vorgaben
- Geregelter Vergabe von Zugriffsrechten bei Eintritt in das Unternehmen
- Entzug von Zugriffsrechten sowie Löschung bzw. Einzug von Schlüsseln bei Austritt
- Zentrale Verwaltung von Zugangsdaten über Bitwarden
- Einsatz aktueller Betriebssysteme (Linux Mint, macOS)

## 10. Löschung und Datenminimierung

- Löschung von Daten innerhalb bereitgestellter Software-Instanzen spätestens 14 Tage nach Vertragsende
- Durchführung der Löschung in der Regel automatisiert
- Speicherung vertriebs- und abrechnungsrelevanter Daten gemäß gesetzlicher Aufbewahrungsfristen
- Speicherung von Supportdaten nur im erforderlichen Umfang
- Löschung temporär bereitgestellter Daten (z. B. im Rahmen von Migrationen) nach Zweckfortfall

## 11. Subunternehmer

- Uberspace (Hosting, Mainz, Deutschland)
- Netcup (Domainverwaltung und E-Mail, Karlsruhe, Deutschland)
- SevDesk (Buchhaltung, Offenburg, Deutschland)
- Die physische Sicherheit der Serverinfrastruktur liegt im Verantwortungsbereich der jeweiligen Anbieter.