



Anlage 1: Technisch-organisatorische Maßnahmen (TOM)

Version 2025.1 – Stand 08.09.2025

1. Zutrittskontrolle

- Arbeitsumgebung ist nicht öffentlich zugänglich; Zutritt nur für berechtigte Personen.
- Zugang zu Büro- und Arbeitsräumen erfolgt ausschließlich über Schlüssel bzw. passwortgeschützte Endgeräte.
- Arbeitsgeräte und Datenträger werden bei Nichtgebrauch sicher verwahrt (abschließbarer Schrank).
- Unbefugten Dritten wird der Zutritt zu Datenverarbeitungsanlagen verwehrt.

2. Zugangskontrolle

- Admin-Accounts und eigene Systeme (z. B. M365, Sophos Central, Zoho Vault) sind durch starke Passwörter und 2-Faktor-Authentifizierung gesichert.
- Der Zugriff auf Kundensysteme erfolgt ausschließlich über individuelle Admin-Zugänge; die Nutzung wird dokumentiert (z. B. im Verzeichnis von Verarbeitungstätigkeiten).
- Gemeinsame Standard-Accounts werden nicht verwendet.

3. Zugriffskontrolle

- Zugriff auf personenbezogene Daten ist auf den vereinbarten Zweck beschränkt und erfolgt ausschließlich nach dem „Need-to-know“-Prinzip.
- Eine Weitergabe von Kundendaten an unbefugte Dritte ist ausgeschlossen.

4. Weitergabekontrolle

- Übermittlung personenbezogener Daten erfolgt ausschließlich verschlüsselt (z. B. TLS, VPN, Fernwartungssoftware mit End-to-End-Verschlüsselung).
- Speicherung personenbezogener Daten auf mobilen Geräten ist nur zulässig, wenn diese durch PIN/Biometrie, Geräteverschlüsselung und Remote-Wipe gesichert sind.
- Für Smartphones ist die Funktion „Mein Gerät finden“ (Android: Google) bzw. „Wo ist?“ (Apple) aktiviert.



5. Eingabekontrolle

- Tätigkeiten im Rahmen der Verarbeitung (z. B. Fernwartungssitzungen oder Vor-Ort-Einsätze) werden dokumentiert.
- Erfasst werden insbesondere Verbindungs- und Einsatzdaten (z. B. Zeit, Dauer, beteiligte Systeme, verantwortliche Person).
- Eine inhaltliche Aufzeichnung von Bildschirmhalten oder Tätigkeiten erfolgt grundsätzlich nicht. Sollte in Ausnahmefällen eine Aufzeichnung für technische Klärungen erforderlich sein, erfolgt dies ausschließlich nach vorheriger ausdrücklicher Zustimmung des Auftraggebers.
- Die Dokumentation erfolgt im Verzeichnis von Verarbeitungstätigkeiten (VVT) und dient der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO.

6. Auftragskontrolle

- Verarbeitung personenbezogener Daten erfolgt ausschließlich auf dokumentierte Weisungen des Auftraggebers.
- Subunternehmer werden nur nach Abschluss einer Vereinbarung zur Auftragsverarbeitung (AVV) und mit Zustimmung des Auftraggebers eingesetzt.
- Die jeweils aktuelle Liste der Subunternehmer ist in **Anlage 2: Liste der Subunternehmer** dokumentiert. Link: <https://digitalservice-kalteis.de/dsgvo-subunternehmer/>

7. Verfügbarkeitskontrolle

- Geschäftskritische Daten (z. B. M365, Buchhaltung, Kundenverwaltung) werden regelmäßig verschlüsselt gesichert.
- Backups erfolgen zusätzlich auf Wechselmedien, die getrennt vom Produktivsystem aufbewahrt werden.
- Wiederherstellungstests werden in angemessenen Abständen durchgeführt.

8. Trennungsgebot

- Kundendaten werden mandantentrennt verarbeitet, soweit Systeme dies technisch vorsehen.



- Rechnungs- und Buchhaltungsdaten werden ausschließlich für den Zweck der Vertrags- und Geschäftsabwicklung in Lexoffice verarbeitet.
- Eine Vermischung von Daten unterschiedlicher Auftraggeber findet nicht statt.