Lehrmeister

Technische und Organisatorische Maßnahmen (TOM) (gem. Art. 32 Abs. 1 DSGVO)

Stand: Juni 2025

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die die Software Werke („Betreiber“) einzurichten und laufend aufrechtzuerhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen.

1) Datenzugriff

Jeder registrierte und somit authentifizierte Nutzer ist nur für die Einsicht seiner eigenen Daten autorisiert. Es gibt keine Möglichkeit, personenbezogene Daten anderer Nutzer einzusehen.

Alle Passwörter werden clientseitig mittels einer kryptografischen Hashfunktion verschlüsselt, bevor sie an den Server übertragen und in der Datenbank gespeichert werden. Alle Anwendungsdaten des Nutzers werden direkt auf dem Endgerät mit dem Passwort des Nutzers verschlüsselt und erst danach zum Server übertragen.

Es ist jedoch grundsätzlich notwendig, dass insbesondere vertragsbezogene Daten, als auch Daten zur Erstellung des Nutzeraccounts nicht vollständig verschlüsselt und für den Betreiber lesbar sind. Daten, die der Nutzer hingegen in der App selbst hochlädt, sind grundsätzlich verschlüsselt.

Die gesamte Kommunikation zwischen Server und Client findet zudem mit dem hybriden Verschlüsselungsprotokoll TLS statt.

Ausschließlich vom Betreiber autorisierte Mitarbeiter haben Zugriff auf anonymisierte Statistiken zu Anzahl und Status der Benutzerkonten (nicht deren Anwendungsdaten). Dies wird über eine Authentifizierung vor unberechtigtem Zugriff geschützt.

Der Zugang zu den Servern ist mit Hilfe einer Public-Key-Infrastruktur abgesichert. Somit kann lediglich der Inhaber des privaten Schlüssels mittels SSH auf die Server und somit die Datenbanken zugreifen. Der Inhaber des privaten Schlüssels ist der vom Betreiber autorisierte Mitarbeiter für Serveradministration.

2) Gewährleistung der Vertraulichkeit

Durch die Ende-zu-Ende-Verschlüsselung werden alle Daten eines Nutzers nur verschlüsselt auf den Servern gespeichert. Damit sind diese vor unbefugtem Zugriff geschützt. Nur der Nutzer kann mit seinem geheimen Passwort seine Daten auf seinem Gerät entschlüsseln und einsehen.

3) Gewährleistung der Integrität

Alle Anwendungsdaten werden automatisiert von der Anwendung des Betreibers auf dem Gerät des Nutzers mit dessen geheimen Passwort verschlüsselt. Die Übertragung zum Server ist zusätzlich mit TLS verschlüsselt. Alle Verschlüsselungsmechanismen basieren auf aktuellen und weit verbreiteten Standards, die die Integrität der Daten gewährleisten. Die verschlüsselten Anwendungsdaten werden niemals verändert und nur durch Löschen des Benutzerkontos vom Server gelöscht.

Alle Daten des Benutzerprofils werden vom Betreiber ausschließlich gelesen, aber niemals verändert und nur durch Löschen des Benutzerkontos vom Server gelöscht.

4) Gewährleistung der Verfügbarkeit

Alle gemieteten und genutzten Server sind nach ISO-27001 zertifiziert.

5) Gewährleistung der Belastbarkeit der Systeme

Alle gemieteten und genutzten Server sind nach ISO-27001 zertifiziert. Alle Geräte, die über SSH auf die Server zugreifen könnten, werden mit Hilfe aktueller Verfahren sicher vor Eindringlingen und Schadsoftware aller Art gehalten.

6) Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Back-up Konzept: Alle gespeicherten Daten werden täglich gesichert und für 14 Tage auf einem separaten Server gespeichert. Einmal pro Woche wird das aktuelle Backup aller Daten auf einem weiteren Server in einem anderen Rechenzentrum gespeichert und für drei Monate gesichert.

7) Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die technischen und organisatorischen Maßnahmen werden regelmäßig geprüft. Die zuständigen Mitarbeiter informieren sich regelmäßig über aktuelle Entwicklungen und prüfen und beraten intern, ob und wenn ja, welche Anpassung erforderlich ist.

8) Interne Verhaltensregeln

Alle Mitarbeiter des Betreibers wurden intern über das Thema Datenschutz unterrichtet und sensibilisiert. Für den Datenschutz angemessene Arbeitsprozesse- und abläufe wurden eingerichtet und etabliert.