# Technische und organisatorische Maßnahmen (TOMs)

myCistern Operations GmbH

## Präambel

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO, die von der myCistern Operations GmbH zum Schutz der verarbeiteten personenbezogenen Daten und der IoT-Telemetriedaten implementiert wurden. Die Infrastruktur wird auf dedizierten Servern innerhalb der Europäischen Union betrieben.

## 1 Vertraulichkeit (Zutritts-, Zugangs- und Zugriffskontrolle)

### Physische Zugangskontrolle (Zutrittskontrolle)

Maßnahmen, die unbefugten physischen Zugang zu den Datenverarbeitungsanlagen verhindern:

- Die Server-Infrastruktur wird in den ISO 27001-zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland gehostet.
- Strikte physische Zugangskontrollen zum Rechenzentrum (biometrische Zugangssysteme, 24/7-Sicherheitsdienst, Videoüberwachung).

### Systemzugangskontrolle (Zugangskontrolle)

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden:

- Der administrative Zugriff auf die Server erfolgt ausschließlich über verschlüsselte Fernwartungszugänge (SSH) unter Verwendung von starken kryptografischen Schlüsseln auf Basis aktueller asymmetrischer Verschlüsselungsverfahren.
- Die direkte Anmeldung als Hauptadministrator (Root-Zugriff) über diese Fernwartungszugänge ist serverseitig vollständig deaktiviert.
- Einsatz von lokalen Firewalls zur strikten Limitierung der von außen erreichbaren Schnittstellen auf das absolute Minimum (wie etwa HTTPS, sicheres MQTT und SSH).

### Datenzugriffskontrolle und Trennung (Zugriffskontrolle)

Maßnahmen, die sicherstellen, dass Berechtigte nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können:

- Logische Trennung der Mandantendaten auf Datenbankebene. Jede Systemabfrage erzwingt die Validierung einer eindeutigen Mandantenkennung, um Datenüberschneidungen auszuschließen.
- Striktes rollenbasiertes Zugriffskontrollsystem innerhalb der Plattform und der Web-Benutzeroberflächen.
- Das Training der lokal gehosteten KI-Modelle erfolgt strikt separiert von der produktiven Datenbank. Dafür werden ausschließlich Daten genutzt, die zuvor automatisierte Prozesse

zur vollständigen Entfernung direkter Identifikatoren sowie zur zeitlichen Vergröberung von Zeitstempeln durchlaufen haben.

# 2 Integrität (Weitergabe- und Eingabekontrolle)

### Datenübertragung (Weitergabekontrolle)

Maßnahmen, die gewährleisten, dass Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die gesamte Kommunikation zwischen IoT-Geräten, Web-Benutzeroberflächen und der Plattform erfolgt verschlüsselt nach aktuellem Industriestandard (TLS 1.2 / TLS 1.3).
- Nutzung von HTTPS für den allgemeinen Web-Verkehr und gesichertem MQTT für die Übertragung der Sensordaten an den zentralen Nachrichtenserver (Broker).

### Eingabevalidierung (Eingabekontrolle)

Maßnahmen zur Sicherstellung der Datenintegrität bei der Eingabe:

- Strikte serverseitige Überprüfung und Validierung aller eingehenden Nutzdaten zur Verhinderung von Schadcode-Einschleusungen (Injection-Angriffen) oder der Verarbeitung beschädigter Telemetriedaten.

# 3 Verfügbarkeit und Belastbarkeit (Verfügbarkeitskontrolle)

### Backup-Strategie

Maßnahmen, die sicherstellen, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Tägliche, verschlüsselte Sicherungsabbilder der Datenbanken und Systemkonfigurationen.
- Die Backups werden auf physisch getrennten Speichermedien innerhalb der Europäischen Union gesichert, um eine räumliche Ausfallsicherheit (Geo-Redundanz auf nationaler Ebene) zu gewährleisten.

### Schutz vor Überlastungsangriffen

- Nutzung der automatisierten Infrastruktur des Hostinganbieters zur frühzeitigen Erkennung und Abwehr von netzwerkbasierten Überlastungsangriffen (DDoS-Schutz).

# 4 Überprüfung und Evaluation

### Patch-Management

Verfahren zur regelmäßigen Überprüfung und Aktualisierung der Systemkomponenten:

- Automatisierte Installation sicherheitskritischer Updates auf dem Host-Betriebssystem mittels systemeigener Update-Routinen.
- Regelmäßiges Monitoring und zeitnahe Aktualisierung aller verwendeten Open-Source-Bibliotheken und KI-Modelle.

### Protokollierung (Logging)

- Zentrale Erfassung und Auswertung von Systemereignissen, Authentifizierungsversuchen und administrativen Änderungen.
- Die Protokolldateien werden nach dem Prinzip der geringstmöglichen Rechte vor unbefugtem Zugriff geschützt und nach Ablauf festgelegter Fristen automatisiert überschrieben (Log-Rotation).