

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMS)

gemäß Art. 32 DSGVO für „Tracar Smart Tracking“

Stand: 2026

Auftragsverarbeiter: MiZeI GmbH

1. ZIEL UND ANWENDUNGSBEREICH

Diese technischen und organisatorischen Maßnahmen (TOMS) beschreiben die von der MiZeI GmbH umgesetzten Sicherheitsmaßnahmen zum Schutz personenbezogener Daten im Rahmen der Nutzung der Tracking-Lösung Tracar Smart Tracking.

Die Maßnahmen dienen insbesondere dem Schutz von:

- Positions- und Bewegungsdaten von Assets,
- daraus ableitbaren personenbezogenen Daten,
- Verfügbarkeit, Integrität und Vertraulichkeit der Systeme.

2. ZUTRITTSKONTROLLE

- Betrieb der Systeme in zertifizierten Rechenzentren innerhalb der EU
- Hosting in der AWS-Region Frankfurt (eu-central-1)
- Physische Zutrittskontrollen durch den Rechenzentrumsbetreiber (mehrstufige Sicherheitskonzepte)
- Zutritt nur für autorisierte Personen
- Protokollierung und Nachvollziehbarkeit von Zutritten durch den Betreiber

3. ZUGANGSKONTROLLE

- Zugriff auf Systeme ausschließlich über personalisierte Benutzerkonten
- Starke Authentifizierungsmechanismen (z. B. Passwort-Richtlinien, ggf. MFA)
- Keine Gruppen- oder Sammelkonten
- Regelmäßige Überprüfung und Entzug nicht mehr benötigter Zugänge
- Schutz vor unbefugter Nutzung durch technische Maßnahmen

4. ZUGRIFFSKONTROLLE (ROLLENBASIERT)

- Rollen- und Rechtemodell nach dem Need-to-know-Prinzip
- Typische Rollen:
 - Administrator (Systemverwaltung)
 - Disponent / Fuhrparkverwaltung
 - Leseberechtigte Nutzer
- Zugriff auf Positions- und Trackingdaten nur, soweit für die jeweilige Rolle erforderlich
- Protokollierung administrativer Zugriffe

5. ZWECKBINDUNG & SCHUTZ VOR LEISTUNGSÜBERWACHUNG

- Verarbeitung von Standort- und Positionsdaten ausschließlich zu objektbezogenen Zwecken
- Keine Verarbeitung zur Leistungs- oder Verhaltensüberwachung von Beschäftigten
- Keine permanente oder lückenlose Überwachung natürlicher Personen
- Technische und organisatorische Maßnahmen zur Einschränkung der Dauer und Granularität der Datenerfassung
- Nutzung außerhalb der Arbeitszeit nur, wenn vom Verantwortlichen entsprechend konfiguriert oder deaktiviert

6. WEITERGABEKONTROLLE

- Keine unbefugte Weitergabe von Daten an Dritte
- Übermittlungen ausschließlich:
 - innerhalb der Anwendung,
 - an vertraglich gebundene Unterauftragsverarbeiter,
 - auf Weisung des Verantwortlichen
- Verschlüsselte Datenübertragung (TLS)
- Schutz vor unbefugtem Export oder Kopieren

7. TRENNUNGSGEBOT

- Strikte Mandantentrennung zwischen Kunden
- Logische Trennung der Daten auf System- und Anwendungsebene
- Keine mandantenübergreifenden Zugriffe
- Separate Lösch- und Exportprozesse je Kunde

8. VERFÜGBARKEITSKONTROLLE

- Redundante Systemarchitektur innerhalb der AWS-Region Frankfurt
- Regelmäßige, automatisierte Backups
- Schutz vor Datenverlust durch technische und organisatorische Maßnahmen
- Überwachung der Systemverfügbarkeit

9. INTEGRITÄTSKONTROLLE

- Schutz vor unbefugter Veränderung von Daten
- Protokollierung relevanter administrativer Änderungen
- Versions- und Änderungsnachvollziehbarkeit
- Einsatz aktueller Sicherheitsupdates und Patches

10. VERSCHLÜSSELUNG

- Verschlüsselte Datenübertragung (TLS)
- Verschlüsselung gespeicherter Daten nach dem Stand der Technik
- Schutz kryptographischer Schlüssel vor unbefugtem Zugriff
- Orientierung an anerkannten Standards (z. B. BSI-Empfehlungen)

11. LÖSCH- UND AUFBEWAHRUNGSKONZEPT

- Speicherung von Positions- und Trackingdaten nur für den erforderlichen Zeitraum
- Löschung oder Anonymisierung gemäß Weisung des Verantwortlichen
- Technisch unterstützte Löschroutinen
- Löschung nach Vertragsende oder Rückgabe an den Verantwortlichen
- Dokumentierte Löschprozesse

12. AUFTRAGSKONTROLLE

- Verarbeitung personenbezogener Daten ausschließlich auf Weisung des Verantwortlichen
- Regelmäßige Schulung der mit der Verarbeitung betrauten Personen
- Verpflichtung auf Vertraulichkeit
- Interne Richtlinien zum Datenschutz und zur Datensicherheit

13. DATENSCHUTZ DURCH TECHNIKGESTALTUNG

- Datenschutzfreundliche Voreinstellungen
- Minimierung der erhobenen Daten
- Konfigurierbare Erfassungsintervalle
- Zweckgebundene Nutzungsmöglichkeiten
- Unterstützung des Verantwortlichen bei der Umsetzung datenschutzkonformer Einstellungen

14. KONTROLLE UND WEITERENTWICKLUNG

- Regelmäßige Überprüfung und Anpassung der TOMs
- Berücksichtigung technischer und rechtlicher Entwicklungen
- Dokumentation wesentlicher Änderungen