

# ANHANG 1: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

der

Next Generation Mobility GmbH & Co. KG  
Baierbrunner Str. 35  
81379 München, Deutschland  
-fleetster-

**Version 2.35**

## Technische und organisatorische Maßnahmen

Für das Vertragsverhältnis zwischen der Next Generation Mobility GmbH & Co KG, mit Sitz in der Baierbrunner Str. 35, 81379 München, Deutschland (nachfolgend "**fleetster**" genannt) und deren Kunden für die Softwareplattform fleetster (nachfolgend "**Kunde**" genannt), gelten die nachfolgenden technischen und organisatorischen Maßnahmen als Teil der **Vereinbarung zur Auftragsverarbeitung** (<https://www.fleetster.de/legal/vereinbarung-auftragsverarbeitung.pdf>).

### I. INHALTSVERZEICHNIS

1.	Technische und organisatorische Maßnahmen .....	3
1.1	fleetster Büro / fleetster intern .....	3
1.2	fleetster Software .....	3

# 1. Technische und organisatorische Maßnahmen

---

## 1.1 fleetster Büro / fleetster intern

Es gibt keine Server im fleetster Büro. Alle Server stehen im Amazon Web Services Rechenzentrum in Frankfurt am Main (Deutschland).

- **Zutrittskontrolle**
  - o Token für Tür im Erdgeschoss (Zugang zum Treppenhaus)
  - o Fingerabdruck-Scanner für Zugang zu den Büroräumen
  - o Besucher werden immer von fleetster-Mitarbeitern begleitet
- **Zugangskontrolle**
  - o Technische Sicherungsanlagen (Büro):
    - G-Data Antivirus
    - Firewall Router
    - MAC Whitelist für LAN und WLAN
- **Zugriffskontrolle**
  - o Authentifizierungs- und Passwort-Richtlinien
  - o Richtlinien zur Arbeitsplatzsicherung
  - o Verschlüsselte Festplatten an Arbeitsplätzen, die Anmeldedaten zu personenbezogenen Daten enthalten
- **Weitergabekontrolle**
  - o Lokales NAS ("network-attached storage")
  - o in Ausnahmefällen: PGP
- **Eingabekontrolle** (nicht zutreffend)
- **Auftragskontrolle** (nicht zutreffend)
- **Verfügbarkeitskontrolle** (nicht zutreffend)
- **Datentrennung** (nicht zutreffend)

## 1.2 fleetster Software

- **Zutrittskontrolle & Zugangskontrolle**

siehe Amazon Web Services Inc.'s (AWS) Dokumente:

  - o <https://aws.amazon.com/compliance/data-center/data-centers/>
  - o <https://aws.amazon.com/compliance/data-center/controls/>
- **Zugriffskontrolle**
  - o Datenbankverschlüsselung
  - o Während der Nutzung kommuniziert die Software nur mit userIDs

*Siehe auch fleetster's IT Security concept*
- **Weitergabekontrolle**
  - o Elektronische Übermittlung von Daten: TLS & HTTPS
- **Eingabekontrolle**
  - o Änderungen/Eingaben v. personenbezogenen Daten direkt in der fleetster Datenbank werden aufgezeichnet, genauso wie externe Zugriffe von Nutzern (Logfile für Logins)

- Die fleetster Datenbank zeichnet Netzwerkzugriff auf, inklusive Zeitstempel und IP Adresse. Auch Zugriff-Versuche werden aufgezeichnet, inklusive Zeitstempel, Nutzername und Zieldatenbank.
  - **Auftragskontrolle**
    - Allgemeine Geschäftsbedingungen & Vereinbarung zur Auftragsverarbeitung
    - Unterauftragnehmer, der personenbezogene Daten hostet: AWS
  - **Verfügbarkeitskontrolle**
    - AWS garantiert eine hochverfügbare Cloud-Infrastruktur
    - Redundanzen & Backups
    - Test-Recoveries
  - **Datentrennung**
    - Trennung von Produktiv-, Entwicklungs- und Testsystemen
- Siehe auch fleetster's IT Security concept*