EXHIBIT 1:

TECHNICAL AND ORGANISATIONAL MEASURES

from

Next Generation Mobility GmbH
Zielstattstr. 13
81379 Munich, Germany
-fleetster-

Document Version 2.36

Technical and organisational measures

The contractual relationship between Next Generation Mobility GmbH, having its registered office at Zielstattstr. 13, 81379 Munich, Germany (hereinafter referred to as "**fleetster**") and its customer for the fleetster software platform ("**Customer**"), is governed by the following technical and organisational measures as part of fleetster's **contract processing of data** (https://www.fleetster.net/legal/contract-processing-of-data.pdf).

I. TABLE OF CONTENTS

1. Technical and organisational measures

1.1 fleetster office / fleetster internal

There are no servers in the fleetster office. All servers are in the Amazon Web Services' data center in Frankfurt a. Main (Germany).

- **Physical access control**
  - Token for door downstairs (access to the staircase)
  - Finger print access to the office
  - Visitors are always supervised by a fleetster employee
  - Camera in entrance area that detects motions outside business hours
- **Logical access control**
  - Technical security systems (office):
    - G-Data antivirus
    - Router Firewall
    - MAC whitelist for LAN and WiFi
- **Data access control**
  - Password policy
  - Workspace security guidelines
  - Encrypted hard disks for work stations containing credentials to personal data
- **Data transfer control**
  - Local NAS (network-attached storage)
  - Exceptions: PGP
- **Entry control** (not applicable)
- **Control of instructions** (not applicable)
- **Availability control** (not applicable)
- **Separation control** (not applicable)

1.2 fleetster software

- **Physical access control & Logical access control**
  See Amazon Web Services Inc.'s (AWS) documents
  - https://aws.amazon.com/compliance/data-center/data-centers/
  - https://aws.amazon.com/compliance/data-center/controls/
- **Data access control**
  - Database encrypted at rest
  - Authentication and authorization
  - Firewall
  - IP-whitelist
  - Client certificates

  Also see fleetster's IT Security Concept
- **Data transfer control**
  - Electronic transfer of personal data: TLS & HTTPS

- **Entry control**
  - Editing / inserting any data directly in a fleetster database is tracked as well as external access (by users) which is tracked in the logfile for logins
  - fleetster's database logs database access, including timestamps and source IP address. Also, authorization attempts are logged, including timestamps, username and target database.
- **Control of instructions**
  - Standard terms and conditions & contract processing of data
  - Only one subcontractor hosts databases with personal data: AWS
- **Availability control**
  - AWS guarantees a highly available cloud system
  - Redundancies & backups
  - Test recoveries & frequent backup checks
- **Separation control**
  - Separation of production, development and testing systems

Also see "data separation" section in fleetster's IT Security Concept