EXHIBIT 1:
TECHNICAL AND ORGANISATIONAL MEASURES

from

Next Generation Mobility GmbH & Co. KG
Baierbrunner Str. 35
81379 Munich, Germany
-fleetster-

Document Version 2.35
The contractual relationship between Next Generation Mobility GmbH & Co. KG, having its registered office at Baierbrunner Str. 35, 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 .................................................................................................................. 3
   1.1 fleetster office / fleetster internal ........................................................................................................................ 3
   1.2 fleetster software ............................................................................................................................................... 3
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

- **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**
  o 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
  o 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**
  o Standard terms and conditions & contract processing of data
  o Only one subcontractor hosts databases with personal data: AWS

• **Availability control**
  o AWS guarantees a highly available cloud system
  o Redundancies & backups
  o Test recoveries & frequent backup checks

• **Separation control**
  o Separation of production, development and testing systems

*Also see “data separation” section in fleetster’s IT Security Concept*