EXHIBIT 1:

TECHNICAL AND ORGANISATIONAL MEASURES

from

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

Document Version 2.40

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. Introduction

1.1 Responsible Party

The responsible party according to Art. 4 No. 7 EU General Data Protection Regulation (GDPR) is Next Generation Mobility GmbH, Zielstattstraße 13, 81379 Munich, Germany, e-mail: info@fleetster.net. We are legally represented by Tim Ruhoff.

1.2 Data Protection Officer

Our data protection officer is heyData GmbH, Kantstr. 99, 10627 Berlin, Germany, www.heydata.eu, e-mail: datenschutz@heydata.eu.

1.3 Subject of the Document

This document summarizes the technical and organizational measures taken by fleetster within the meaning of Article 32 (1) of the GDPR. These are measures with which fleetster protects personal data. The purpose of the document is to assist fleetster in fulfilling its accountability obligations under Art. 5(2) GDPR.

2. Confidentiality (Art. 32 (1) (b) GDPR)

2.1 Physical Access Control

The following implemented measures prevent unauthorized persons from gaining access to data processing facilities:

- Automatic access control system
- Biometric access barriers
- Chip card/transponder locking system
- Visitors only accompanied by employees

See also Amazon Web Services EMEA SARL (AWS) Documents:

- *https://aws.amazon.com/compliance/data-center/data-centers/*
- *https://aws.amazon.com/compliance/data-center/controls/*

2.2 Data Access Control

The following implemented measures prevent unauthorized persons from accessing data processing systems:

- Authentication with user and password
- Use of anti-virus software
- Use of VPN technology for remote accesses
- Automatic desktop lock
- Use of 2-factor authentication
- Firewall router
- MAC whitelist for LAN and WLAN

- Authentication and password policies
- Workstation security policies
- Encrypted hard drives at workstations that contain credentials to personal information

See also Amazon Web Services EMEA SARL (AWS) Documents:

- *https://aws.amazon.com/compliance/data-center/data-centers/*
- *https://aws.amazon.com/compliance/data-center/controls/*

See also fleetster's IT Security Concept

2.3 Access Control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Use of document shredders (with cross cut function)
- Use of an authorization concept
- Number of administrators is kept as small as possible
- Customer database is behind a so-called "bastion host
- Access requires user name, password and security certificate

2.4 Separation Control

The following measures ensure that personal data collected for different purposes is processed separately:

- Separation of productive and test system
- Encryption of data records processed for the same purpose
- Logical client separation (on the software side)
- Creation of an authorization concept
- Definition of database rights

See also fleetster's IT Security Concept

3. Integrity (Art. 32 (1) (b) GDPR)

3.1 Transfer Control

It is ensured that personal data cannot be read, copied, changed or removed without authorization during transfer or storage on data carriers and that it is possible to verify which persons or bodies have received personal data. The following measures are implemented to ensure this:

- Installation of VPN tunnels
- WLAN encryption (WPA2 with strong password)
- Electronic transmission of data: TLS & HTTPS

- in exceptional cases: PGP

3.2 Input Control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Clear responsibilities for deletions
- Changes/inputs of personal data directly in the fleetster database are recorded, as well as external accesses of users (logfile for logins)
- The fleetster database records network access, including time stamp and IP address. Access attempts are also recorded, including timestamp, user name and target database.

4. Availability and Resilience (Art. 32 (1) (b) GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Fire extinguishers in server rooms
- Fire and smoke detection systems
- Regular backups
- Creation of an emergency plan
- Regular data recovery tests and logging of results
- No sanitary facilities in or above the server room
- Hosting with a professional hoster (AWS guarantees a highly available cloud infrastructure)
- Redundancies & backups
- Test recoveries

5. Procedures for regular Review, Assessment and Evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

5.1 Data Protection Management

The following measures are intended to ensure that an organization that meets the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Commitment of employees to data secrecy
- Regular training of employees in data protection
- Keeping an overview of processing activities (Art. 30 GDPR)

5.2 Incident-Response-Management

The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches:

- Notification process for data protection breaches pursuant to Art. 4 No. 12 DSGVO vis-à-vis the supervisory authorities (Art. 33 DSGVO).
- Notification process for data protection breaches pursuant to Art. 4 No. 12 DSGVO vis-à-vis the data subjects (Art. 34 DSGVO)
- Involvement of the data protection officer in security incidents and data mishaps
- Use of anti-virus software

5.3 Data Protection-Friendly Default Settings (Art. 25 (2) GDPR)

The following implemented measures take into account the requirements of the "Privacy by design" and "Privacy by default" principles:

- Training of employees in "Privacy by design" and "Privacy by default".
- No more personal data is collected than is necessary for the respective purpose.

5.4 Order Control

The following measures ensure that personal data can only be processed in accordance with instructions:

- Written instructions to the contractor or instructions in text form (e.g. by order processing contract).
- Ensuring that data is destroyed after completion of the order, e.g. by requesting appropriate confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially with regard to data security)