Data protection agreement for the processing of data in accordance with the German Federal Data Protection Act (BDSG) and EU General Data Protection Regulation (EU GDPR)

between

Felyx E-scooters 1 BV

Herengracht 493

1017 BT Amsterdam, Netherlands

- hereinafter referred to as the Client -

and

fleetbird GmbH
Hansastr. 95
44137 Dortmund, Germany

- hereinafter referred to as the Contractor -

1. Subject matter and duration of the order
1.1 The subject matter of the order results from the "DE_Softwarevertrag" or "Software license agreement" (hereinafter: Main Contract).
1.2 The term of the order results from the Main Contract mentioned above.

2. Clarification of the contractual content
2.1 The scope, nature and purpose of the collection, processing or use of personal data by the Contractor for the Client can be described as follows: The personal data will be processed to ensure a smooth sharing operation of the vehicle fleet. In this way, trips, invoices, and other customer activities can be reproduced and used for further processing.
The contractually agreed data processing shall take place exclusively within a Member State of the European Union, or in another state that is party to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Client, and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

2.3 The types of personal data used are the following: *personal master data, communications data (e.g., telephone, email), contract master data (tariff, contractual relationship, product or contractual interest), customer history, driver's license information, contract billing data, planning and control data, information (from third parties, e.g., credit agencies, or from public directories).*
2.4 The categories of persons affected by the processing are: *Customers, employees, contacts, suppliers.*

3. Technical and organizational measures
3.1 The Contractor shall document the implementation of technical and organizational measures set out prior to the placing of an order before the start of processing, particularly with regard to the specific order execution, and shall provide this to the Client for review. Upon Client acceptance, the documented measures shall become the

JH

basis of the Contract. If the Client's review/audit results in a need for adjustment, this must be implemented by mutual agreement.

3.2 The Contractor must provide the security pursuant to § 9 BDSG and Art. 28 para. 3 lit. c, Art. 32 GDPR, in particular in conjunction with Art. 5 para. 1 para. 2 GDPR. Overall, the measures to be taken are data security measures and are taken to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. On this point, the state of the art, the costs of implementation, the nature, scope and purposes of processing, and the varying likelihood and risk severity for the rights and freedoms of natural persons in the sense of Art. 32 (1) 1 GDPR is to be taken into account (cf. Annex).

3.2 Technical and organizational measures are subject to technical progress and further developments. In that regard, the Contractor is permitted to implement alternative adequate measures. The security level of the specified measures must be adequate. Significant amendments are to be documented.

4. Correction, restriction and deletion of data

4.1 The Contractor may not rectify, erase or restrict the processing of the Client's data that is processed on behalf of the Client on its own authority, but only in accordance with documented instruction from him. If a person concerned contacts the Contractor directly in this regard, the Contractor shall immediately forward this request to the Client.

4.2 Insofar as the scope of services includes, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the Contractor in accordance with the documented instructions of the Client.

5. Controls, quality assurance and other obligations of the Contractor

The Contractor has additional legal obligations under Art. 28 to 33 GDPR to comply with the provisions of this order; in this respect, he guarantees particular compliance with the following requirements:

5.1. Written appointment - to the extent required by law - of a data protection officer who performs his/her duties in accordance with §§ 4f, 4g BDSG or Art. 38 and Art. 39 Federal Data Protection Act.

5.2. Maintaining confidentiality in accordance with § 5 Federal Data Protection Act and Art. 28 para. 3 lit. b, Art. 29, Art. 32 para. 4 GDPR. In carrying out work, the Contractor shall exclusively use employees who are bound to confidentiality, and who have previously been familiarized with the relevant data protection provisions. The Contractor and any person under his/her control who has access to personal data may process such data exclusively in accordance with the instructions of the Client, including the powers granted in this Contract, unless they are legally obliged to process it.

5.3. The implementation and observance of all technical and organizational measures required for this contract in accordance with § 9 Federal Data Protection Act or Art. 32 GDPR.

5.4. On request, the Client and the Contractor shall cooperate with the supervisory authority in the performance of their duties and shall inform each other thereof without delay. This also applies to investigations within the scope of administrative offenses and criminal proceedings as well as to liability claims of affected persons or third parties or other claims in connection with order processing.

5.5. The Contractor shall regularly monitor internal processes and technical and organizational measures to ensure that processing within his area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.

5.6. Verifiability of the technical and organizational measures taken vis-a-vis the Client within the scope of his control authority in accordance with No. 7 of this Contract.

6. Subcontracting relationships

6.1 Sub-contracting relationships within the meaning of this provision shall be understood to mean those services that relate directly to the provision of the main service performance. This does not include ancillary services which the Contractor uses, e.g., as telecommunication services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor shall be obliged to undertake appropriate and legally binding contractual agreements and control measures to ensure the data protection and the data security of the Client's data, including in the case of outsourced ancillary services.

6.2 The Contractor may only commission subcontractors (other contractors) with the express prior written or documented consent of the Client.

□ The Client agrees to the assignment of the following subcontractors under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR:

1. Amazon Web Services, Inc. ; 410 Terry Ave North ; Seattle , WA 98109-5210 , USA
   a. Server location: Frankfurt (EU)

The outsourcing to subcontractors or the change of the existing subcontractor is permitted, insofar as:

a) the Contractor notifies the Client of such outsourcing to subcontractors in writing or in text form in advance and
b) the Client does not object to the planned outsourcing in writing or in text form until the time of handover of the data to the Contractor and
c) a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is used as a basis.

6.3 The transfer of the Client's personal data to the subcontractor and commencement of his initial activities are only permitted if all requirements for subcontracting are met.

6.4 If the subcontractor performs the agreed service outside the EU/EEA, the Contractor shall take appropriate measures to ensure the admissibility under data protection law. The same applies if service providers will be used within the meaning of para. 1 sentence 2.

(5) Any further outsourcing by the subcontractor requires the express consent of the main client (at a minimum, in writing).

7. Client's Controlling Rights

7.1 The Client has the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be appointed in individual cases. He has the right to conduct periodic random checks, which, as a rule, must be notified in good time, to ensure compliance with this Agreement by the Contractor in his business operations.

7.2 The Contractor shall ensure that the Client is not obliged to comply with the obligations of the Contractor pursuant to § 11 para. 2 sentence 4 Federal Data Protection Act or Art. 28 GDPR. The Contractor is required to furnish the necessary information to the Client on request and to demonstrate in particular the implementation of the technical and organizational measures.

7.3 Proof of such measures, which not only concern the specific order, can be provided by

- compliance with approved rules of conduct referred to in Art. 40 GDPR.
- certification according to an approved certification procedure according to Art. 42 GDPR

- current certificates, reports or report extracts from independent bodies (e.g., auditors, Review, data protection officers, IT security department, data protection auditors, quality auditors)
- appropriate certification with an IT security or data protection audit (e.g., pursuant to BSI-basic protection).

7.4 The Contractor can assert a claim for remuneration for enabling the Client to carry out inspections.

8. Communication in the event of violations by the Contractor

8.1 The Contractor shall support the Client in complying with the obligations specified in § 42a Federal Data Protection Act and Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data leaks, data protection impact assessments and prior consultations. These include, but are not limited to:

a) Ensuring an adequate level of protection by means of technical and organizational measures, that consider the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a possible infringement due to vulnerabilities and make an immediate identification of relevant violations possible
b) The obligation to report violations of personal data to the Client without delay
c) The obligation to support the Client in the context of his duty to inform the person concerned and to make all relevant information available to him in this connection without delay
d) The support of the Client for his data protection impact assessment
e) Supporting the Client in prior consultations with the supervisory authority

8.2 The Contractor is entitled to remuneration for support services that are not included in the service specifications or are attributable to inappropriate behavior of the Contractor.

9. Client's authority to Issue Instructions

9.1 The Client confirms verbal instructions without delay (at a minimum, in text form).

9.2 The Contractor must inform the Client immediately if he is of the opinion that an instruction violates data protection regulations. The Contractor is authorized to suspend implementation of the corresponding instruction until it is confirmed or modified by responsible client personnel.

10. Deletion and return of personal data

10.1 Copies or duplicates of data may not be created without the Client's knowledge. This excludes backups, if they are necessary to ensure proper data processing, as well as data that are required in order to comply with legal retention requirements.

10.2 Upon completion of the contract work or earlier, if requested by the Client – but no later than termination of the Service Agreement - the Contractor shall hand over to the Client all documents which have come into his possession, drafted processing and user results and all data resources that are related to the contractual relationship, or destroy them in line with data protection regulations, with prior consent. The same applies to testing and excess material. The log of the deletion must be submitted upon request.

10.3 Documentation that serves as proof of order-compliant and proper data processing must be kept by the Contractor in accordance with the respective retention periods beyond the term of the Agreement. However, for his own relief, the Contractor may also return them to the Client at the end of the Agreement.

For the Contractor: For the Client:

Contractor

Place, Date Dortmund 25.05.18
Name 10.2.e
Function
Signature COO Floatbird

10.2.e

Client Felyx E-scooters 1 BV

Place, Date Amsterdam 25-5-2018
Name 10.2.e
Function Co-founder
Signature

10.2.e

10.2.e

Appendix: Technical and organizational measures by the Contractor

according to § 9 Federal Data Protection Act or Art. 32 GDPR
(No. 3 of the privacy agreement)

1. Confidentiality (Art. 32 para. 1 letter b GDPR)

1.1 Access control
An unauthorized access is to be prevented where the term is to be understood spatially.
- Access control system: RFID chip
- Documented allocation of keys
- Key allocation/access authorization only for full/part-time/research assistants
- Door security (electric door opener, etc.)
- Locking rooms after conclusion of the work day
- Guests are always accompanied and welcomed inside the office building
- Access control by authorized persons (e.g., by staff of the co-working area)
- Surveillance equipment: alarm system, video surveillance (not in the offices), motion detector

1.2 Access control
The entry of unauthorized persons into IT systems is to be prevented.
- Servers can only be used after an individual login
- Clients can only be used after an individual login
- Login with password procedures (including special characters, minimum length)
- Automatic blocking during pauses, IP spam and incorrect logons (e.g., password or pause switching)
- Set-up of a user master record per user
- Standard routines for regular updating of protection software
- Encryption of data media

1.3 Access Control
Unauthorized activities in IT systems beyond granted permissions are to be prevented.
- There is an authorization concept with different privileges (profiles, roles, transactions and objects)
- Release/approval procedure defined for assigning authorizations
- Number of administrators largely reduced (can be influenced by the Client)
- Use of secure deletion methods
- Logging of information, changes, deletion of data
- Evaluation capabilities

1.3 Separation control
Data collected for different purposes must also be processed separately.
- Internal multi-client capability (e.g: data of different customers is logically/physically separated)
- Functional separation (production/test)
- Areas of competence and responsibility are clearly defined

1.4 Use of pseudonyms (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)
A personal reference is only possible if additional information can be added.

- Personal data is only stored under a pseudonym (e.g., reference ID), as far as this is possible during processing or transmission to third-party systems.
- The additional information which may establish a personal reference is kept encrypted

2. Integrity (Art. 32 para. 1 letter b GDPR)

2.1. Disclosure control
Aspects of the disclosure of personal data is to be regulated: electronic transmission, data transmission, transmission control
- Encrypted lines (SSL etc.)
- Logging
- Sending password-protected files by email

2.2. Input control
The traceability and documentation of data management and maintenance must be ensured.
- Logging and log analysis
- Traceability of input, modification, and deletion of data by individual user names (not user groups)
- Control data are stored

3. Availability and dependability (Art. 32 para. 1 letter b GDPR)

3.1. Availability control
The data must be protected against accidental destruction or loss. Here you have to refer to the hosts and their services (aws.amazon.com)
- Backup and recovery procedures
- Mirroring of hard disks, e.g. RAID methods
- Use of uninterruptible power supply (UPS)
- Separate/disaster-safe storage of backups
- Use of protection programs (virus scanners, firewalls, encryption programs, spam filters), emergency plan is available

4. Procedures for periodic review, assessment and evaluation (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

4.1 Data Protection Management
The data protection management refers to the periodic review, assessment and evaluation of risks, technical and communicative processes, as well as other order-related necessary topics in relation to the processing of data.
Fleetbird has set up internal mechanisms to ensure the proper protection of data in a 2-way system:
1. Over periods of four to six weeks, procedures and internal processes including infrastructure, logs (technical protocols), storage methods, access rights, etc., are discussed in team meetings, reviewed for timeliness and safety tested and in case of doubt, measures to improve the situation are agreed.
2. Current systems are controlled through "real time" monitoring controls, especially with respect to the availability, failure, partial logs, etc. In this way, individuals can

be made aware at short notice regarding any problems and countermeasures to be taken.

4.2 incident response management
No dedicated procedure is set up, as this is part of the normal work process. In the event of data protection incidents, this is the top priority of the management and will be communicated to the Contractor immediately, and countermeasures initiated.

4.3 Default privacy settings (Art. 25 para. 2 GDPR)
By default and through appropriate technical and organizational measures, it shall be ensured that only personal data, the processing of which is required for the particular specific processing purpose, is processed.

4.4 Order control
It muse be ensured that order data processing only occurs according to instructions.

- Unambiguous drafting of contracts
- Formalized order placement (order form)
- Criteria for selecting the Contractor
- Control of contract execution