Last Mile Solutions

Software as a Service Agreement - Contractual Terms

Data Processing Agreement

DATA PROCESSING AGREEMENT

LAST UPDATE: Version v.06.2026

INTEGRAL PART OF : Software as a Service (SaaS) Agreement between Threeforce B.V. acting under the trade name Last Mile Solutions (the Service Provider) and the Purchaser.

This **Data Processing Agreement** is concluded by and between:

1. The Purchaser party to a SaaS agreement with the Service Provider, acting as a Data Controller,

   and

2. The Service Provider, Threeforce B.V., acting under the trade name Last Mile Solutions, a private limited liability company, with head office in Rotterdam and offices in (3016 CN) Rotterdam on Zeemansstraat 11, listed in the Trade Register of the Chamber of Commerce of Rotterdam under number 24360819, acting as a Processor.

The Data Controller and the Processor are hereinafter jointly referred to as "**Parties**" and each separately as a "**Party**".

WHEREAS:

- The Data Controller processes Personal Data and determines the purposes for and the means of the processing of the personal data and therefore qualifies as data controller;
- In connection with the Agreement of the Parties it is necessary to regulate processing of Personal Data (whose controller is the Data Controller or its Affiliates, if applicable) by the Processor;
- In case the Affiliates authorized to use the Service are data controllers of the personal data, the intention of the Parties is that the Data Controller entrusts such personal data on their behalf;
- The Processor shall process personal data under the instruction of the Data Controller without acting under its direct authority and therefore will qualify as a data processor;
- The Data Controller verifies and confirms that the Processor provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subjects;
- The Parties do not intent to include the sensitive data (special categories of data) within the scope of processing under this agreement and the Data Controller will not transfer such data to the Processor, unless otherwise agreed in advance by amendment to this agreement;
- The Parties wish to set out the terms and conditions of this data processing agreement ("**DPA**");

THE PARTIES HAVE AGREED AS FOLLOWS:

ARTICLE 1 DEFINITIONS

Terms used in this Data Processing Agreement that start with a capital letter, have the meaning defined in the Agreement. In addition, or as deviation from the definitions given in the Agreement, the following definitions given in italics below shall apply:

AP	Data Protection Authority of the seat of the Data Controller within the meaning of article 51 and article 56 GDPR.
Data, Personal Data	Personal data within the meaning of article 4 point 1 GDPR whose controllers are Data Controller, entrusted under this Data Processing Agreement to the Processor in connection with services rendered under the Main Agreement.
Data Breach	Means a breach of security within the meaning of article 4 point 12 GDPR and further specified in articles 33-34 GDPR.
Data Subjects	The natural persons to whom the Personal Data relate.
End-User	End-User within the meaning of the Main Agreement.
GDPR	Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Main Agreement	Software as a Service Agreement concluded by and between the Parties.
Process or Processing	Any operations or set of operations which is performed on Personal Data or on sets of Personal Data within the scope of this DPA, whether or not by automated means.
Security Measures	The security measures which must be implemented by the Processor as described in this DPA.
Ticket	A manual or automated document created in the Platform to request support. The ticket contains specific information: ticket ID, Sign-on date, Last action on date, created by, source, charge point ID, charge point, Customer ID (if applicable) Customer (if applicable), User group (if applicable), Action holder (if applicable), Description (if applicable), Action taken (if applicable). Personal information is only used when this information is needed to resolve the request.

ARTICLE 2 PURPOSE OF PROCESSING THE PERSONAL DATA

2.1. The Processor is only permitted to process the Personal Data on behalf of the Data Controller in accordance with the documented instructions and under the supervision of the Data Controller, unless required to do so by law to which the Processor is subject; in such a case, the Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor has no control (in Dutch: 'zeggenschap') over the purposes for and means of the Processing of the Personal Data.

The Parties agree that instructions of the Data Controller may be given in writing, via e-mail, as well as otherwise, digitally, which involves inter alia instructions provided via Admin Account at the Platform, by way of choosing functionalities, configurations or settings.

2.2. The purpose of the Processing by the Processor and its sub-processors is to perform the Main Agreement, including services and activities necessary under the Main Agreement to be conducted by the Processor, to provide access to the Platform, to manage and maintain the Platform and provide support, as well as securing such performance. The Processor shall process the Personal Data only for this specific purpose.

2.3. In case the Data Controller purchases the automatic billing module Service as described in the Main Agreement, Parties act as independent controllers for the purposes connected with the subject matter of the Partial Transfer and specifically: (i) invoicing End-Users; (ii) collecting revenue for Charging Services and other services for End-Users; (iii) reimbursing employees of End-Users for within Home Charging Reimbursement Service.

2.4. The nature of Processing, type of Personal Data, as well as categories of Data Subjects, whose Personal Data are processed under this DPA, are indicated in Annex 1 hereto.

2.5. This DPA shall apply to all Personal Data processed by the Processor for the purpose indicated above, including:

a. all Personal Data extracted by the Processor for Processing;
b. all Personal Data transmitted to the Processor for Processing;
c. all Personal Data accessed or otherwise received by the Processor on the authority of the Data Controller for Processing; and
d. all Personal Data otherwise received by the Processor for Processing on the Data Controller's behalf.

The Personal Data remains to be the possession of the Data Controller and/or the Data Subject.

2.6. In case the list of Data Controller's Affiliates is attached hereto, this shall be interpreted as entering into this DPA by the Data Controller also on behalf of such Affiliates. In such a case the rights of Affiliates as data controllers hereunder are executed by the Data Controller as their authorized representative. The Data Controller shall represent the Affiliates concerning their rights to inspect, modify and/or destroy the Personal Data. All the notifications and other duties of the Processor hereunder towards the Affiliates shall be executed towards the Data Controller as their authorized representative. In such a case:

a. This DPA shall be interpreted as applicable to the Affiliate(s) meaning that all clauses applicable to the Data Controller rights or duties of or towards the Data Controller shall be treated as analogicaly applicable to the Affiliates, as well as any authorization, consent or declaration made by the Data Controller shall be treated as made also on behalf of the Affiliate being a party hereto (if applicable).
b. The Data Controller shall immediately inform the Processor in case its authorization to act on behalf of any of the Affilitates is revoked. In such a case the Data Controller shall ensure that the new authorization is given, or this DPA is terminated to the extent concerning such an Affiliate. In such a case the Processor shall be also authorized to immediately terminate this DPA with such respective Affiliate.
c. The Data Controller shall ensure that for the whole term of this DPA it is authorized to represent the Affiliates also to the extent necessary to execute their rights as the data controllers within the meaning of the GDPR hereunder and being notified with the legal effects towards such Affiliates hereunder.
d. This DPA shall be terminated in relation between the Processor and respective Affiliate if the Affiliate or the Data Controller stops to be authorized to access the Services of the Processor rendered under the Main Agreement, irrespective of the reason therefor.

In case no list of Affiliates of the Data Controller is added hereto, this DPA will be treated as concluded only in its own name by the Data Controller. Future changes in this regard require concluding additional data processing agreement or amending this DPA by the way of addendum.

ARTICLE 3 OBLIGATIONS OF THE PROCESSOR

3.1. At the first request of the Data Controller to inspect, modify and/or destroy the Personal Data, the Processor is obligated to cooperate with the Data Controller.

3.2. The Processor is obligated to comply with the applicable law and regulations, including the GDPR.

3.3. The Processor is obligated to maintain a record of all categories of processing activities carried out on behalf of the Data Controller, containing:

a. the name and contact details of the Processor or any (sub-)processors and of the Data Controller on behalf of which the Processor is acting, and where applicable, the representative and the Data Protection Officer of the Data Controller and/or the Processor;
b. the categories of processing carried out on behalf of the Data Controller;
c. where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards;
d. a general description of the technical and organizational security measures referred to in this DPA;
e. At first request of the Data Controller, the Processor is obligated to inform the Data Controller regarding the measures the Processor has implemented in respect of the obligations under this DPA.

3.4. The Processor is obligated to impose its obligations under this DPA on all the parties and persons who act under the authority of the Processor, including its employees and any (sub-)processors.

3.5. The Processor undertakes to grant written authorizations to Processing of Personal Data to all persons who will Process the entrusted data to perform this DPA.

3.6. The Processor undertakes to ensure the confidentiality of Processed Personal Data by persons who are authorized to the Processing of Personal Data for the purpose of implementing this DPA, also after termination of the DPA. The Processor shall ensure that these natural persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.7. The Processor is obligated to inform the Data Controller immediately if, in its opinion, an instruction from the Data Controller infringes the GDPR and/or other applicable data protection provisions. The Processor shall immediately inform the Data Controller if it is unable to follow such instructions.

3.8. The Processor is obligated to provide all cooperation that the Data Controller can reasonably expect that is necessary for carrying out an assessment of the impact of the processing on the

rights and freedoms of natural persons (also called 'Data protection impact assessment'), any time when such an assessment is required by law.

3.9. The Processor is obligated to provide all cooperation that Data Controller can reasonably expect in consulting the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk.

3.10. If the Processor becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the Data Controller without undue delay. In this case, the Processor shall cooperate with the Data Controller to erase or rectify the Data.

ARTICLE 4 SECURITY MEASURES

4.1. The Processor shall take adequate technical and organizational measures to protect the Personal Data against accidental or unlawful loss, destruction, modification or any form of unauthorized disclosure, unauthorized access to Personal Data or other unjustified Processing, as required by article 32 GDPR.

To this end, you can contact us to obtain, among other things, the reports and certifications achieved (ISO 9001:2015, ISO/IEC 27001:2022, and ISO/IEC 27701:2019) as well as the related documentation by reaching out to us at the following address: security@lastmilesolutions.com.

4.2. When transferring the Personal Data to the Processor, the Data Controller is obliged to implement appropriate technical and organizational measures to ensure the security of such Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data. Taking into account the nature of processing and the information available to the Processor, the Processor shall assist the Data Controller in ensuring compliance with the Controller's obligations in relation to the security of Personal Data.

ARTICLE 5 NOTIFICATION REQUIREMENT IN CASE OF DATA BREACHES

5.1. Only the Data Controller shall assess whether there is a Data Breach. The Processor shall enable the Data Controller to make such an assessment in a timely and adequate manner. In the event of a suspected Data Breach, the Processor shall immediately, but at least within 24 hours after becoming aware of the suspected Data Breach, inform the Data Controller in writing thereof on the email address indicated in the Main Agreement and shall provide to the Data Controller all available information that the Data Controller may need to assess whether there is a Data Breach. If the Data Controller requests the Processor to provide (additional) information to assess whether there is a Data Breach, the Processor shall provide the requested information as soon as reasonably possible, but at least within 24 hours after the request.

5.2. The Processor shall as soon as reasonably possible, but at least within 24 hours after becoming aware of the suspected Data Breach, provide Data Controller with the information needed for making a notification as meant in article 33 GDPR which includes at least the following information:

a. the Personal Data involved;
b. the nature of the Data Breach;
c. the categories and approximate number of Data Subjects concerned;
d. the categories and approximate number of Personal Data records concerned;

e. the period in which the Data Breach occurred;
f. the likely consequences of the Data Breach;
g. a description of the actual and suspected negative consequences of the Data Breach;
h. the measures taken and/or proposed by the Processor to address the Data Breach, including measures to mitigate the possible adverse effects of the Data Breach;
i. the name and contact details of the Data Protection Officer or other contact point of Data Controller where more information can be obtained.

5.3. Only the Data Controller itself shall notify the AP or any other supervisory authority (if such authority is competent in such a case) and, if necessary, the Data Subjects about a Data Breach. Without the prior written consent of the Data Controller the Processor is not entitled to notify the AP or any other supervisory authority (if such authority is competent in such a case) and/or the Data Subjects in case of Data Breaches.

ARTICLE 6 TRANSFER OF PERSONAL DATA

6.1. Without the prior written consent of the Data Controller, the Processor is not allowed to provide (access to) Personal Data to any third parties, unless it is necessary and inevitable to fulfill the Main Agreement.

6.2. The Parties may transfer Personal Data outside the EEA, Switzerland, or the UK to perform the Main Agreement. Such transfers must be to jurisdictions recognized as providing with an adequate level of protection pursuant to an adequacy decision protection under data protection laws or, if unavailable, appropriate safeguards like Standard Contractual Clauses must be implemented

ARTICLE 7 CONTROL AND AUDIT

7.1. At least once a year, or promptly at the first request of the Data Controller, the Data Controller is entitled to audit the compliance with the obligations of the Processor under this DPA. The Processor is obligated to provide all cooperation that the Data Controller may reasonably expect. The Data Controller is entitled to appoint a qualified professional for the performance of the audit.

7.2. The Parties shall mutually agree on the date of the audit. The audit may take place on the business premises of the Processor. The Data Controller will ensure that an audit will cause as little disturbance as possible to the business activities of the Processor and will ensure strict confidentiality of the confidential data of the Processor disclosed to him during the audit.

7.3. To carry out an audit in accordance with this article, the Processor is obligated to establish and maintain adequate administration, bookkeeping and archives for these purposes. The Processor is obligated to organize and manage its bookkeeping and archives in accordance with the applicable market standards.

ARTICLE 8 AUTHORITIES

8.1. The Processor recognizes the competence of the AP and/or other competent (supervisory) authorities to:

a. obtain information from the Processor and/or from parties that are engaged by the Processor in relation to the Processing of Personal Data; and/or

b. conduct investigations relating to the business operations and processes in relation to the Processing of Personal Data;

c. The Processor is obligated to fully cooperate with such requests. The Processor shall ensure that third parties and its (external) accountants who are engaged by the Processor also fully cooperate with such requests.

8.2. The Processor shall immediately notify the Data Controller, at least within twenty-four (24) hours, if the AP and/or other (supervisory) authority contacts the Processor to obtain information and/or to investigate in relation to the Processing of Personal Data. Where permissible under the law, the Processor agrees in particular to notify the Data Controller if it receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data Processed pursuant to this DPA or if it becomes aware of any direct access by public authorities to such Personal Data.

ARTICLE 9 RIGHTS OF DATA SUBJECTS

9.1. The Processor is obligated to inform the Data Controller immediately, and at least within twenty-four (24) hours, if a Data Subject has filed a request to exercise his or her rights under the GDPR in connection with the Processing of their Personal Data under this DPA.

9.2. The Processor agrees to assist the Data Controller with all information requests which may be received from any Data Subject in relation to any Personal Data.

9.3. The Processor will only communicate with the Data Subjects and handle requests as referred to in article 9.1 above, after prior written consent of the Data Controller.

9.4. Upon termination of the Main Agreement, the Processor shall delete Tickets older than three (3) months from its own platform. The same applies if the respective Affiliate (if any) stops being authorized to access the services rendered by the Processor under the Main Agreement. All unresolved Tickets will follow the termination of the Main Agreement as soon as they are resolved.

ARTICLE 10 CONFIDENTIALITY

10.1. The Processor is required to keep all Personal Data strictly confidential.

10.2. Without the prior written consent of the Data Controller, the Processor is not allowed to communicate to third parties, including but not limited to the Data Subjects, supervisory authorities and/or the media, about any information that is related to this DPA and/or to a Data Breach, unless the Processor is required – under the law – to do so.

ARTICLE 11 LIABILITY

11.1. The Processor is liable to the Data Controller for damages caused by an attributable failure in the performance of its obligations as a Data Processor pursuant to the present DPA and to GDPR. Liability of the Processor for improper performance of this DPA shall be governed by article 8 of the Main Agreement.

ARTICLE 12 DURATION

12.1. This DPA shall enter into force upon the date of signing thereof by the Parties and shall continue for the duration of their cooperation under the Main Agreement, or at least as long as the Processor processes the Personal Data on behalf of the Data Controller under this DPA. This DPA shall be terminated and authorization to Process Personal Data on behalf of the Data Controller shall expire upon termination, dissolution or expiry of the Main Agreement.

12.2. Article 10 (Confidentiality), article 11 (Liability), article 12 (Duration), article 13 (Effect of termination) and article 18 (Applicable law and dispute resolution) shall survive for an indefinite period after the termination or dissolution of this DPA.

ARTICLE 13 EFFECT OF TERMINATION

13.1. In the event the Processor still retains Personal Data after the termination of this DPA, the Processor will destroy these Personal Data as soon as possible, or – upon first request of the Data Controller - return the Personal Data to the Data Controller, unless the Processor is required to retain the Personal Data based on applicable laws and/or regulations. In the latter case, the Processor will fulfill all obligations under this DPA throughout the period in which the Processor is obligated to retain the Personal Data under applicable law or regulation.

ARTICLE 14 APPOINTMENT OF (SUB-)PROCESSORS

14.1. Subject to point 14.2, without the prior written consent of the Data Controller, the Processor is not allowed to appoint any (sub-)processors for the Processing of Personal Data.

14.2. Annex 2 of this DPA, available at the following URL : https://legal.lastmilesolutions.com/hubfs/legal/Subprocessors/Subprocessors%20list.pdf, lists all the subcontractors being sub-processors used by the Service Provider at the date of signature of this DPA and authorized by the Data Controller i.e., the Data Controller grants its specific written authorization for engaging another processor within the meaning of Article 28 sec. 2 of the GDPR. The Data Controller grants also its general consent to engage other subcontractors for the purpose of processing the personal data entrusted hereunder from the following categories: entities that provide services used in connection with the Main Agreement, as well as other Affiliates of the Processor and authorize further entrusting Personal Data to such subcontractors i.e. the Data Controller grants its general written authorization for engaging another processor within the meaning of Article 28 sec. 2 of the GDPR. In this case the following procedure shall apply:

a. In the event of planned engagement of the further subcontractor, planned changes or replacements of the subcontractors Processing Personal Data (including the ones listed in Annex 2 "Authorized Subcontracting", available at the following URL : https://legal.lastmilesolutions.com/hubfs/legal/Subprocessors/Subprocessors%20list.pdf), the Processor shall provide the Data Controller with the advance notice including the full name of the planned subcontractor and all details as required under Annex 2, as well as the planned date of further entrusting processing of personal data to such subcontractor (not less than ten (10) working days in advance);

b. If no objections are notified in writing within ten (10) working days of the notification of the update of the list of subcontractors - further processors, the Processor shall be entitled to entrust processing of personal data hereunder to such a subcontractor;

c. If the Data Controller reasonably objects to any such subcontractor, it shall notify the Processor of such objections in writing within ten (10) working days of the notification of

the update of the list of subcontractors - further processors. In such a case Parties shall seek to resolve the matter in good faith and discuss options that may be available. If the use of a subcontractor is necessary for the provision of the Services under the Main Agreement and Parties do not find any amicable solution that would cause the Data Controller to withdraw its objections within a further ten (10) business days after notification of the objections, the Parties agree that:

(1) the Data Controller shall be entitled to terminate this Agreement together with the Main Agreement by serving formal notice to the Processor by registered letter with acknowledgement of receipt at thirty (30) days' notice;

(2) if the Data Controller has not terminated the Agreement together with the Main Agreement within the next ten (10) business days in accordance with this subsection (iii) above, the objections of the Data Controller shall be deemed as withdrawn and the Processor shall be entitled to entrust processing of personal data hereunder to such a subcontractor in question and continue to provide Services with its engagement.

d. The Processor shall ensure that (sub-)processors are bound by written agreements that require them to comply with corresponding obligations to those contained in this DPA.

e. At the request of the Data Controller, the Processor shall provide the Data Controller with a copy of the contract it has concluded with the (sub-)processor and, in the event of changes, provide the Data Controller with its updated version.

f. Any affiliates of the Processor, as defined under the Main Agreement, will be recognized as sub-processors of the Processor. The Affiliates acting as sub-processors will refrain from processing Personal Data for any purposes other than those specified in the Main Agreement, unless otherwise required by applicable laws.

ARTICLE 15 OBLIGATIONS OF THE DATA CONTROLLER

15.1. The Data Controller shall cooperate with the Processor in the performance of this DPA, shall provide the Processor with explanation in case of doubts concerning legality of the Data Controller's instructions and comply with the Data Controller's obligations in a timely manner.

15.2. The Data Controller shall immediately inform the Processor about any administrative or judicial proceedings, regarding the processing of Personal Data and about any administrative decision or ruling addressed to the Data Controller - if it affects the performance of this DPA.

15.3. If the Data Controller receives a request in the scope of exercising the rights of Data Subjects under the provisions of Chapter III of GDPR ("Rights of the data subject"), the performance of which affects this DPA, in particular the scope or manner of processing of the Personal Data by the Processor, the Data Controller shall immediately inform the Processor about it, adjusting at the same time the instructions, authorizations or instructions previously provided to the Processor.

ARTICLE 16 COSTS

16.1. Costs arising from (access) requests from Data Subjects, investigations and/or audits by the Data Controller, AP or another (supervisory) authority in relation to Personal Data being a subject of this DPA, will be borne by the Data Controller, unless in the event of material findings in the investigations and/or audits conducted at the Processor's premises.

16.2. Direct costs arising from requests or seizures by judicial authorities at the Processor shall be borne by the Processor.

ARTICLE 17 CHANGE IN LAWS AND/OR REGULATIONS

17.1. The Processor is obligated to provide all reasonable assistance to the Data Controller, including but not limited to any reasonable requests to amend this DPA, on the basis of changes in any applicable laws and/or regulations.

ARTICLE 18 APPLICABLE LAW AND DISPUTE RESOLUTION

18.1. This DPA will be governed and construed in accordance with the laws of the Netherlands.

18.2. All disputes arising in connection with this DPA, shall be exclusively brought before the competent court in Rotterdam, the Netherlands. The Parties agree that a Data Subject may also bring legal proceedings against the Data Controller, or the Processor before the courts of the member state in which he/she has his/her habitual residence, and they agree to submit themselves to the jurisdiction of such courts.

Purchaser:

_____

Service Provider:

Threeforce B.V.
Mr. Arie Albertus (Eric) van Voorden - CEO

_____

ANNEX NO. 1. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS, MEANS AND CHARACTER OF THE PERSONAL DATA PROCESSING

Categories of Data Subjects	Categories of Personal Data	Means of Personal Data processing	Nature of Personal Data Processing
End Users of the Data Controller and Affiliates (if any) i.e. EV Drivers, CSO, CPO, Fleet EV Drivers or other, including beneficiaries of services e.g., employees of the End User accessing the Account from the End-User, End-User's personnel using the service	Normal data (not sensitive Personal Data): name, surname, customer reference (if applicable), customer cost centre number (if applicable), license plate (if applicable), contact details (phone number, e-mail address), data on charging, including RFID card/token number/ID, energy consumption, charging history including localization of charging, possessed charging infrastructure, job position, logins, passwords, log in history, User group (if applicable).	In electronic form (Platform)	Collecting Recording Storage Protection of data Correcting, Modifying, Deleting, Accessing, Disclosing to third parties in connection with the performance of the Main Agreement
End Users of the Data Controller and Affiliates (if any) requesting for support	E-mail address, name and phone number, ticket number, ticketID, Sign-on date, Last action on date, created by, source, charge point ID, charge point, Customer ID (if applicable) Customer (if applicable), User group (if applicable), Action holder (if applicable), Description (if applicable), Action taken (if applicable).	In electronic form (Platform)	Collecting Recording Storage Protection of data Correcting, Modifying, Deleting, Accessing, Disclosing to third parties in connection with the performance of the Main Agreement

Additional information on Processing of Personal Data under the DPA:

Sensitive Personal Data: No

Personal Data of the persons under 16 years old: No

Retention: Data will be retained for up to three months after the termination of the Main Agreement.

ANNEX NO. 2. AUTHORIZED SUBCONTRACTING

Available at the following URL : https://legal.lastmilesolutions.com/hubfs/legal/Subprocessors/Subprocessors%20list.pdf

Available on demand at the following adress : privacy@lastmilesolutions.com

ANNEX NO. 3. SWISS ADDENDUM

ARTICLE 1 SWISS APPLICATION AND INTERPRETATION

This Addendum apply to personal data subject to Swiss data protection law, whether Swiss data protection law applies alone or together with the GDPR. "Swiss data protection law" means the Swiss Federal Act on Data Protection of 25 September 2020, its implementing ordinances, and any law that amends, replaces, or re-enacts them. Where Swiss data protection law applies, references to the GDPR include the corresponding requirements under Swiss data protection law, and references to the EU, EEA, Member States, EU or EEA supervisory authorities, and EU or EEA regulators include and/or are replaced by Switzerland and the Federal Data Protection and Information Commissioner, where the context permits.

If this clause conflicts with another term, the term that gives stronger protection to data subjects will apply, unless Swiss data protection law requires a different result.

ARTICLE 2 SWISS PROCESSING AND DISCLOSURES

For personal data subject to Swiss data protection law, the processing details are those described in the DPA, and the associated privacy policy. If personal data is disclosed from Switzerland to a country or recipient not recognised by Switzerland as providing adequate protection, the disclosing party will use a transfer mechanism recognised under Swiss data protection law, unless an exception under that law applies. Customer is responsible for any notification to the Federal Data Protection and Information Commissioner required from Customer or Customer Affiliates under Swiss data protection law.