LIGHTLY.AI GTC | DATA PROTECTION ANNEX

1 DEFINITIONS

1.1 As used in this Annex, capitalised terms, in their singular or plural form, shall have the meanings specified in Article 12.

1.2 The terms "data subject", "processing", "controller" respectively "controller of the data file" and "processor" used in this Annex shall have the meanings specified in the GDPR or Swiss Data Protection Legislation, depending on their respective scope of application.

2 INTRODUCTION

2.1 **Subject matter**. This Annex reflects the agreement between the Parties regarding the terms governing the processing and security of Customer Data under the Agreement.

2.2 **Term**. This Annex shall become effective upon signing of the Agreement and shall remain in effect until the last of the following to occur: (i) the end of the provision of the Services by Provider under the Agreement, including, if applicable, during any period after termination of the Agreement during which Provider continues to provide Services on a transitional basis, or (ii) the deletion of all of Customer Data by Provider in accordance with this Annex (the **Term**).

2.3 **Order of precedence**. In the event of a conflict or inconsistency between the terms of this Annex and the terms of any applicable Agreement, the terms of this Annex shall take precedence.

3 DATA PROTECTION LEGISLATIONS

3.1 **Applicable legislations**. The Parties acknowledge and agree that the following data protection legislations may, depending on the circumstances, apply to the processing of Customer Personal Data:

(a) the GDPR;
(b) Swiss Data Protection Legislation; and/or
(c) Other Applicable Data Protection Legislation.

3.2 **Applicability of this Annex**. Unless otherwise stated in this Annex, the provisions of this Annex shall apply regardless of the legislation applicable to the processing of Customer Personal Data.

4 DATA PROCESSING

4.1 Roles and compliance

4.1.1 Responsibility of the processor and the controller / controller of the data file. If the GDPR or the Swiss Data Protection Legislation apply to the processing of Customer Personal Data, the Parties acknowledge and agree that:

(a) the subject matter and details of the processing are specified in this Annex;
(b) Provider is a processor of Customer Personal Data under the GDPR or the Swiss Data Protection Legislation, as applicable;
(c) Customer is a controller (respectively, controller of the data file), or a processor for a third party, as the case may be, of these Customer Personal Data under the GDPR or the Swiss Data Protection Legislation, as applicable; and
(d) each Party shall comply with its obligations under the GDPR and/or Swiss Data Protection Legislation with regard to the processing of Customer Personal Data.

4.1.2 Authorisation by a third-party controller. If Customer is a processor for a third party, Customer guarantees to Provider that Customer has obtained the express prior authorisation of the applicable controller to Customer's instructions and actions regarding the Customer Personal Data, including the designation of Provider for performance of the Services as another processor.

4.1.3 Other legislation. If Other Applicable Data Protection Legislation applies to the processing of the Customer Personal Data, Customer undertakes to Provider to comply with the obligations applicable to it with regard to the processing of the Customer Personal Data and to inform Provider in writing of any provisions contained in such legislation that could have an impact on the processing of the Customer Personal Data by Provider as a processor for Customer.

4.2 Scope of processing

4.2.1 Nature and purpose of processing. Provider shall process the Customer Personal Data for the purpose of providing the Services and the related technical support to Customer in accordance with the Agreement and, in particular, this Annex.

4.2.2 Instructions by Customer. By entering into the Agreement, Customer instructs Provider, and undertakes to instruct Provider, to process the Customer Personal Data only in strict compliance with applicable law and furthermore:

(a) if the GDPR applies, only to provide the Services and the related technical support as documented (i) in an Agreement, including this Annex, or (ii) in any other manner in writing; and
(b) if the Swiss Data Protection Legislation applies to the processing of the Customer Personal Data, only with regard to processing operations that Customer would be entitled to carry out itself and provided that no legal or contractual obligation to keep the information secret prohibits Provider's involvement.

4.2.3 Provider's compliance with instructions. Provider undertakes to comply with the instructions specified in Section 4.2.2 unless a legislation applicable to Provider requires other processing of Customer Data by Provider.

4.3 Categories of personal data and data subjects

4.3.1 If the GDPR applies to the processing of Customer Personal Data by Provider, information relating to the categories of personal data and data subjects must be included in the Agreement pursuant to which Provider carries out such processing.

4.3.2 Customer undertakes to provide Provider and to keep up to date a list of the categories of Customer Personal Data to which Provider may have access during the provision of the Services, as well as a list of the categories of data subjects. These lists shall constitute an integral part of the Agreement.

4.3.3 Provider disclaims all liability for Customer's failure to provide such information in a timely manner.

4.4 **Obligations of Customer**

4.5 Customer shall be responsible, namely, for the quality, lawfulness and relevance of its personal data processed in the context of the Services and shall be liable to third parties affected by the processing and to the competent data protection authorities. In particular, Customer undertakes to:

(a) provide sufficient information to the data subjects about the collection and processing of their personal data;

(b) obtain the valid consent of the data subjects to the processing of their personal data, if such consent is required under applicable data protection legislation; and

(c) ensure compliance with all rights of the data subjects (e.g. right of access and rectification, right to object etc.) as well as all obligations towards the competent data protection authorities (e.g. declaration of files) under the applicable data protection legislation and regulations.

5 DELETION OF DATA

5.1 **Deletion during the Term**. Provider shall permit Customer to delete or modify the Customer Personal Data during the term of the Agreement [provided such deletion is compatible with the functionality of the Services.]

5.2 **Deletion at the end of the Agreement**. Customer irrevocably requires Provider to delete all Customer Data (including any existing copies) from Provider's systems at the end of the Agreement, in accordance with applicable law. Provider shall comply with this instruction as soon as possible, unless Provider is required to retain all or part of Customer Data for technical or legal reasons. Customer acknowledges and accepts that it is its sole responsibility to transfer and/or safeguard Customer Data that it wishes to keep thereafter.

6 DATA SECURITY

6.1 Security measures

6.1.1 Security measures of Provider. Provider shall implement and maintain appropriate technical and organisational measures to protect Customer Data against the occurrence of Security Incidents. These measures include in particular:

(a) the use of firewalls;

(b) the pseudonymisation and encryption of personal data;

(c) the means to ensure the ongoing confidentiality, integrity, availability and resiliency of processing systems and services;

(d) the means to limit access to Customer Data to personnel who need to access it in the course of providing the Services;

(e) the means to restore the availability of and access to Customer Personal Data within an appropriate time frame in the event of a Security Incident; a procedure to regularly test, analyse and evaluate the effectiveness of technical and organisational measures to ensure the security of the processing.

(f) a procedure to regularly test, analyse and evaluate the effectiveness of technical and organisational measures to ensure the security of the processing.

6.1.2 Security compliance by Provider's personnel. Provider shall take appropriate measures to ensure compliance with the above-mentioned security measures by its employees and subcontractors, in particular by ensuring that all persons authorised to handle Customer Personal Data are committed to maintain confidentiality or are subject to an appropriate legal obligation of confidentiality.

6.2 Security Incidents

6.2.1 Notification of Security Incidents to Customer. If Provider becomes aware of a Security Incident, Provider undertakes to inform Customer as soon as possible by any useful means (in particular via the contact person designated by Customer). Provider shall, to the extent possible, describe the nature of the Security Incident, as well as any measures taken by Provider to mitigate potential risks and the measures that Provider recommends Customer take. The actions of Provider in connection with this Section 6.3 shall not constitute, and shall not be construed as, an admission by Provider of any fault or liability in connection with the Security Incident that has occurred.

6.2.2 Obligations of Customer. Provider will not review the content of Customer Data for the purpose of identifying the type of data involved. Customer shall be solely responsible for carrying out any analysis of Customer Data and for complying with the legal provisions applicable to it, in particular any obligations of Customer to provide a notification of the Security Incident to any competent authority and/or the data subjects. In this context, Provider shall provide Customer with any assistance reasonably required by Customer in order to comply with its obligations.

6.3 **Information on and audits of the security measures**

6.3.1 Information. If the GDPR applies to the processing of Customer Personal Data, Provider shall make available to Customer, in addition to the information contained in the Agreement, including this Annex, all documents and information reasonably necessary to demonstrate Provider's compliance with the GDPR and its obligations arising

therefrom.

6.3.2 Right of audit. Provider shall allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Provider's compliance with its obligations under the GDPR. Provider shall provide reasonable assistance with respect to the audits described in this Section 6.3.2. Upon conclusion of the audit, Customer shall forward the complete audit report to Provider, free of charge.

6.3.3 Request. Any request under Sections 6.3.1 (Information) or 6.3.2 (Audits) must be communicated to Provider in writing and indicate (i) the Customer Personal Data concerned, (ii) the reasons for which the conditions referred to in Sections 6.3.1 (Information), respectively 6.3.2 (Audits) apply to these data, (iii) the specific documents to be reviewed, respectively the specific obligations of Provider to be audited, and (iv) that Customer expressly undertakes to use the information collected only to ensure that Provider is in compliance with its obligations with regard to the Customer Personal Data and in particular that the information collected will not be used in connection with any legal or administrative proceedings against Provider. Unless there are exceptional circumstances, Customer may not make more than one request per year.

6.3.4 Exercise of rights. Upon receiving a request in accordance with the preceding Section, and provided that all conditions are met, Provider shall comply with the request as follows:

(a) Provider shall inform Customer, with regard to the review of documents (Section 6.3.1 [Information] above), of the period during which it may consult the documents at Provider's offices. Unless otherwise expressly agreed by Provider, Customer shall not be authorised to make copies of the documents consulted. Alternatively, Provider may decide to provide the documents by any other useful means, in particular by sending them electronically;

(b) Provider shall inform Customer with regard to audits (Section 6.3.2 [Audit] above) of (i) the date or dates on which the audits may take place and (ii) the scope of the audit, in particular the inspections that may be carried out, in order to check Provider's compliance with its obligations under this Annex. Customer's internal costs or the costs of the independent auditor appointed by it shall be borne entirely by Customer. Provider may invoice Customer for its own costs associated with the preparation for and execution of the audit based on the costs incurred by Provider. Provider may object to any independent auditor appointed by Customer if, in the opinion of Provider, the auditor is not sufficiently qualified, is a competitor of Provider, or in any other way would not be able to perform its duties properly. In this case, Customer may either carry out the audit itself or propose another auditor to Provider.

6.4 Confidential information. The provisions contained in this Section 6.3 shall not be interpreted as requiring Provider to provide Customer with (i) any information relating to trade secrets of Provider or any information of a confidential nature or (ii) any information concerning customers of Provider (except Customer). Provider may make the review of documents (Section 6.3.1 [Information] above) or the conduct of an audit (Section 6.3.2 [Audits] above) subject to the conclusion of a specific confidentiality agreement.

7 SERVICE PROVIDER ASSISTANCE

7.1 **Compliance**. Provider shall provide Customer with all the necessary information so that Customer can demonstrate compliance with its obligations under the GDPR or Swiss Data Protection Legislation. Customer also undertakes to provide Provider with all necessary information to enable Provider to demonstrate compliance with its obligations under the GDPR or Swiss Data Protection Legislation.

7.2 **Requests from data subjects**. If Provider receives a request from a data subject regarding Customer Personal Data, Provider shall direct the data subject to submit its request to Customer, and Customer shall be responsible for responding to all such requests. The Parties agree that it is the sole responsibility of Customer to respond to requests from data subjects.

7.3 **Actions by Customer**. Provider shall, subject to the payment by Customer of its internal and external costs, assist Customer in complying with its legal obligations to the data subjects to the extent reasonable and compatible with the functionality of the Services. The measures shall cover all rights of the data subjects under applicable data protection law, in particular access, rectification, limitation, objection, erasure and portability of their Customer Personal Data.

7.4 **Impact assessments and prior consultation**. If the GDPR applies to the processing of the Customer Personal Data, Provider undertakes, to the extent it can reasonably be expected to do so in light of the nature of the processing and the information available to it, subject to the payment of its internal and external costs, to assist Customer in ensuring its compliance with its impact assessment and prior consultation obligations pursuant to Articles 35 and 36 GDPR.

8 DATA TRANSFERS

8.1 **Authorised countries**. Customer agrees that Provider shall retain and process Customer Data in Switzerland and the European Union, or in any country that has been recognised by the European Commission and Switzerland as ensuring an adequate level of personal data protection and in which Provider or one of its subcontractors maintain facilities.

8.2 **Special authorisation**. Provider shall inform (unless Provider is under a legal obligation not to disclose) Customer prior to any transfer of Customer Personal Data to a country not specified in Section 8.1 above and Customer undertakes to authorise such transfer provided that Provider can

guarantee by any useful means an adequate level of protection for the Customer Personal Data. Transfers to countries identified in the subcontractors list specified in Section 9.1 are deemed approved by Customer.

9 SUB-DELEGATION

9.1 **Consent**. Customer specifically authorises Provider to use subcontractors, which may be Affiliated Entities of Provider or other third parties. Provider undertakes to inform Customer in advance and in writing of any planned changes with respect to the addition or replacement of other subcontractors, in order to permit Customer to raise objections against any such subcontractors.

9.2 **Requirements**. Provider undertakes, in the event of a delegation in accordance with Section 9.1 above, to ensure in writing that:

(a) the subcontractor will only access and process Customer Data to the extent necessary to perform its obligations; and

(b) the subcontractor has contractual obligations to Provider that are at least equivalent to those of Provider to Customer arising from this Annex; and

(c) if the GDPR applies, the obligations set forth in Article 28(3) of the GDPR have been imposed on the subcontractor.

9.3 **Objection**. If the GDPR applies, Customer shall have 30 days after being informed of the planned addition or replacement of a subcontractor (including the name and location of the applicable subcontractor and the activities it will perform) to submit its objections. If Provider confirms the appointment of the subcontractor to Customer, Customer shall be entitled to terminate the applicable Agreement with immediate effect by written notice sent within 14 days of receipt of Provider's confirmation. This termination right shall be Customer's sole and exclusive remedy in the event of an objection to a new subcontractor. Customer's failure to react within any of the deadlines specified in this Section 9.3 shall be deemed an acceptance of the new subcontractor.

10 REGISTER OF PROCESSING ACTIVITIES

10.1 Customer acknowledges that Provider may be required, in particular by the GDPR, to:

(a) collect and store certain information, including the name and contact details of each processor and/or controller with whom Provider acts and, where applicable, the local representative of the controller and/or the data protection officer as well as the categories of processing carried out; and

(b) make such information available to any competent authority.

10.2 Customer undertakes to provide Provider with all information reasonably necessary for Provider to meet its obligations.

11 CUSTOMER CONTACT FOR DATA PROTECTION MATTERS

11.1 **Customer data protection officer**. If the GDPR requires Customer to appoint a data protection officer, Customer must provide that person's contact details to Provider. Provider is required to keep the contact details of Customer's data protection officer in a register of processing activities. By not providing Provider with the contact details of a data protection officer, Customer confirms to Provider that it is not obliged to appoint one.

11.2 **Contact person**. If the GDPR does not require Customer to appoint a data protection officer, Customer may still provide Provider with the contact details of its person in charge of data protection matters. This person shall be Provider's primary point of contact for all data protection communications, thus promoting faster and more efficient information sharing.

11.3 **Igor Susmelj, Officer for the protection of Provider's data**. All communications to be made to Provider relating to this Annex and/or data protection shall be addressed to Igor Susmelj, dataprotection@lightly.ai.

12 DEFINITIONS

12.1 **Affiliated Entity** means any entity controlling, controlled by, or under common control with, a Party. For the purposes of this definition "control" means: (i) ownership of at least 50% of the entity's capital; (ii) ownership of at least 50% of the voting rights within the entity; or (iii) the power to exercise decisive influence over the management of the entity.

12.2 **Agreement** has the meaning specified in the GTC.

12.3 **Annex** means this annex.

12.4 **Customer** has the meaning specified in the GTC.

12.5 **Customer Data** means the data (i) transmitted by Customer to Provider, collected by Provider (from Customer or from third parties on behalf of Customer) in connection with the provision of the Services and (ii) that are held or processed by Provider.

12.6 **Customer Personal Data** means data of a personal nature or personal data, i.e. any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more elements specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, according to and in accordance with the data protection laws applicable to such data, contained in Customer Data.

12.7 **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

12.8 **GTC** means the General Terms & Conditions of Provider, in their latest version applicable between Provider and Customer.

12.9 **Other Applicable Data Protection Legislation** means all data protection legislation other than the Swiss Data Protection Legislation and the GDPR.

12.10 **Provider** has the meaning specified in the Agreement.

12.11 **Services** means all Services provided by Provider to Customer under the Agreement.

12.12 **Security Incident** means a security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of Customer Data or unauthorised access to Customer Data.

12.13 **Swiss Data Protection Legislation** means the Swiss Federal Data Protection Act and its implementing ordinances.

12.14 **Term** has the meaning set forth in Section 2.2.

* * *