DATA PROCESSING AGREEMENT

1. DEFINITIONS

1.1 In this data processing agreement (with its exhibits, addenda and appendices, the "**DPA**"), capitalized terms and expressions shall have the meaning given hereinbelow or, if such terms and expressions are not defined herein, in the Agreement(s):

"Affiliates" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

"Agreement(s)" means the commercial agreement(s) between Customer and LumApps pursuant to which the Protected Data are, or may be, processed. This could be, amongst others, a professional services agreement, or a software-as-a-service agreement.

"Applicable Laws" means the GDPR.

"**Control"** means having the ability to control the management of a company (including the power to appoint or dismiss the majority of the members of the administrative, management or supervisory bodies of that company), exercise a majority of the voting rights in a company or exercise a dominant influence over a company and **"Controlling"** and **"Controlled"** will be construed accordingly.

"Data Subject" means the individual to whom Protected Data relates.

"GDPR" means the European Union's General Data Protection Regulation of the European Parliament and of the Council of 27 April 2016 (Regulation (EU) 2016/679).

"**Personnel"** means LumApps' employees, contractors, and agents, and any other third party engaged by LumApps or acting on LumApps' behalf, other than Sub-processors

"**Processing"** means any operation or set of operations performed upon Protected Data whether or not by automated means. The terms **"processes"**, **"process"** and **"processed"** shall be construed accordingly.

"**Protected Data"** means any information relating to any identified or identifiable natural person, such as Customer's personnel, customers, subcontractors, partners or any other third party (including third parties' personnel), or otherwise qualifying as **"personally identifiable information"**, **"personal information"** or **"personal data"** or similar terms pursuant to Applicable Laws, in each case to the extent disclosed, provided to or otherwise made available to LumApps by, on behalf of, Customer or any Authorized User (as defined in the Agreement(s)) under or in connection with the Agreement(s).

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Protected Data.

"Service" means the subscription services or any services, or any component or combination thereof, provided by LumApps to the Customer as described in the Agreement(s).

"Sub-processor" means any entity (including LumApps' Affiliates) engaged by LumApps to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement(s) or this DPA, insofar as such an entity processes Protected Data on behalf of LumApps.

1.2 Clause, schedule and paragraph headings shall not affect the interpretation of this DPA.

1.3 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.4 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.5 A reference to a statute or statutory provision shall include all subordinate legislation made under that statute or statutory provision.

1.6 A reference to writing or written excludes fax but includes email.

1.7 References to clauses and schedules are to the clauses and schedules of this DPA; references to paragraphs are to paragraphs of the relevant schedule to this DPA.

2. PROCESSING OF PROTECTED DATA

Description and means of Processing

2.1 Insofar as LumApps will be processing Protected Data on behalf of the Customer in the course of the performance of the Agreements with the Customer, the terms of this Data Processing Agreement shall apply. A description of the applicable processing operations (including the nature of

Protected Data, categories of Data Subjects, and the nature and purposes for which the Protected Data are being processed) is provided in Addendum A.

2.2 LumApps shall process Protected Data in accordance with written instructions provided by Customer and this DPA; provided that in no event shall LumApps be required to process, or liable for not processing, Protected Data in accordance therewith if, in LumApps' reasonable opinion, the relevant instruction provided by Customer or provision of this DPA infringes Applicable Laws.

2.3 LumApps shall exercise its sole and absolute discretion in the selection and use of the means of processing as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this Data Processing Agreement, in particular the Customer's written instructions.

Customer's right to provide Protected Data

2.4 The Customer represents and warrants that it has all necessary rights to provide the Protected Data to LumApps for the Processing to be performed in relation to the Services, and that one (or more) lawful base(s) set forth in Applicable Laws support(s) the lawfulness of the Processing. To the extent required by Applicable Laws, the Customer is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and, unless another legal basis set forth in Applicable Laws supports the lawfulness of the Processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consents is properly maintained. Should such a consent be revoked by a Data Subject, the Customer shall promptly inform and provide instruction to LumApps accordingly, and LumApps shall implement the Customer's instructions with respect to the Processing of that Protected Data.

LumApps' compliance with laws

2.4 LumApps shall comply with Applicable Laws to the extent applicable thereto in its quality of **"data processor"** or similar terms (as defined in Applicable Laws) and maintain reasonably accurate records of the Processing of Protected Data.

2.5 Attached to this DPA are addenda that provide terms specific to the Processing of Protected Data arising out of specific legal requirements from particular jurisdictions. In the event of a conflict or inconsistency between this DPA and an Addendum, the Addendum applicable to Protected Data from the relevant jurisdiction shall prevail with respect to Protected Data from that relevant jurisdiction, but solely with regard to the portion of the provision in conflict or that is inconsistent.

3. COOPERATION

Requests from Data Subject and authorities

3.1 In the event that any request from either Data Subjects to exercise their rights under Applicable Laws or authorities having jurisdiction over Data Subjects' Protected Data is made directly to LumApps, LumApps shall refrain from responding to such communication directly without Customer's authorization; provided that LumApps may, at its sole and absolute discretion, inform the requestor that LumApps is not authorized to respond directly to a request, and recommend the requestor submit the request directly to Customer; provided, further, that in no event shall the foregoing prevent LumApps to respond to any request to the extent that LumApps is legally compelled to reply thereto. LumApps shall provide reasonable assistance to the Customer by taking appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights under the Applicable Laws.

Data protection impact assessments

3.2 Taking into account the nature of the Processing and information available to LumApps, LumApps shall provide any and all information regarding the Services reasonably requested by Customer to enable Customer to carry out data protection impact assessments or similar evaluations and assessments if required by Applicable Laws.

Relations with authorities

3.3 LumApps shall provide reasonable assistance to Customer in the cooperation or prior consultations with supervisory authorities or other competent regulatory authorities having jurisdiction over Protected Data.

Complaints

3.4 In the event that LumApps receives any official complaint, notice, or communication that relates to Customer's compliance with Applicable Laws in connection with Protected Data, LumApps shall promptly notify Customer and shall reasonably cooperate with Customer as Customer may request in connection therewith.

Communications regarding Security Incident

3.5 Customer shall have sole and absolute discretion as to whether any notifications will be made following a Security Incident involving Protected Data. LumApps shall reasonably cooperate with Customer efforts to notify affected or potentially affected Data Subjects, regulatory authorities and/or third parties, where deemed by Customer to be required by Applicable Laws.

4. CONTRACTING WITH SUBPROCESSORS

List of Sub-processors

4.1 The list of the Sub-processors engaged by LumApps for purposes of the Processing of Protected Data (the "**List of Authorized Sub-processors**") is available online on:

https://www.lumapps.com/legal/lumapps-platform-subprocessors

LumApps is hereby authorized to engage the Sub-processors listed in the List of Authorized Sub-processors (the "**Authorized Sub-processors**"), as amended from time to time, for the Service-related Data Processing activities described in Addendum A.

4.2 LumApps shall inform the Customer of any addition or replacement of the Authorized Sub-processors. The Customer shall be entitled to object to the engagement of a new Sub-processor in accordance with Applicable Laws and in any event within ten (10) days after being notified of such engagement. If the Customer sends a written objection notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve the Customer's objection. In the absence of a resolution, LumApps will make commercially reasonable efforts to provide the Customer with the same level of service described in the Agreement, without using the Sub-processor to process Customer's Protected Data. If LumApps' efforts are not successful within a reasonable time, each Party may terminate the portion of the Service which cannot be provided without such Sub-processor.

Sub-processors' compliance

4.3 LumApps shall procure that each Sub-processor complies with the terms of this DPA as if it were a party in lieu-and-place of LumApps and will be liable for the acts of its Sub-processors that would be a breach of LumApps' obligations hereunder, had such acts been made by LumApps.

5. SECURITY OF PROTECTED DATA

Security measures

5.1 LumApps agrees to implement and maintain appropriate technical and organizational measures to secure Protected Data from Security Incidents and to preserve the confidentiality, integrity, and availability of Protected Data, all in accordance with relevant industry standards. These measures shall include, at a minimum, the security measures set out in Addendum B. Notwithstanding any provision to the contrary, LumApps may modify or update the physical, technical and organizational security measures at its sole and absolute discretion; provided that such modification or update does not result in a material degradation in the protection offered by the physical, technical and organizational security measures.

Audits

5.2 At the request of the Customer, LumApps shall provide reasonable evidence that it complies with its obligations under this Article 5. The Customer shall be permitted, on giving at least 30 days' notice to LumApps and at the Customer's cost, to carry out, or have carried out by a third party who has entered into a confidentiality agreement in terms reasonable satisfactory to LumApps, an audit of the information reasonably necessary to ensure compliance of LumApps with its obligations defined under this Article 5; provided that in no event shall the Customer be entitled to carry out, or have carried out, more than one audit per year. LumApps shall cooperate with such audits carried out by or on behalf of the Customer and shall grant the Customer´s auditors reasonable access to any devices and systems involved with the Processing of the Protected Data. LumApps shall provide the Customer and/or the Customer´s auditors with access to any information relating to the Processing of the Protected Data as may be reasonably required by the Customer to ascertain the LumApps' compliance with this Data Processing Agreement.

Changes in the security measures

5.3 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. LumApps will therefore evaluate the measures as implemented in accordance with this Article 5 on an on-going basis in order to maintain compliance with the requirements set out in this this Article 5. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements required by data protection authorities of competent jurisdiction or Applicable Laws.

6. DURATION AND TERMINATION

Term

6.1 This DPA shall come into effect on the effective date of the Agreement and remain in force so long as LumApps is processing Personal Data on behalf of the Customer under or in connection with the Agreement.

Deletion of Protected Data

6.2 Upon expiration or termination of the Agreement, LumApps shall, at the Customer's costs and expenses, make available and/or delete the Protected Data within 180 days thereafter, unless Applicable Laws require, otherwise and in any case subject to the terms of the Agreement.

7. GENERAL TERMS

Confidentiality

7.1 LumApps undertakes and agrees to:
a) to retain and handle Protected Data with the same level of

protection and caution as LumApps uses to protect its own Personal Data;

b) not to disclose, in whole or in part, the Protected Data to any third party;

c) to use the Protected Data for the sole purpose of performance of the Services and for no longer than is necessary;

d) to only disclose the Personal Data to those of its directors, officers, employees and advisors who have a need-to-know such Protected Data for purposes consistent with this DPA in which case LumApps shall: (i) advise such directors, officers, employees and advisors of the confidential nature of the Protected Data; and (ii) the obligations set out in this DPA; and

e) to immediately cease, on prior, express and written request of the Customer, any use of the Protected Data and to return or to destroy the documents or supporting information containing the Protected Data as well as any reproduction of the Protected Data.

Government Requests to Access Protected Data

7.2 If any authority requires LumApps to procure access to Protected Data relating to Customer or a Data Subject, LumApps will make reasonable endeavors to redirect the relevant authority to request such access directly from Customer. If compelled to provide such access, LumApps shall, to the extent legally permitted, give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy.

Updates to the DPA

7.3. In the event of changes to Applicable Laws (including the amendment, revision or introduction of new laws, regulations, or other legally binding requirements to which either Party is subject), the Parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any addenda.

Conflict of terms

7.4. In the event of conflict between the terms of this DPA and the Agreement(s), the terms of this DPA shall prevail to the extent of that conflict in connection with the Processing of Protected Data.

Applicable law and competent court

7.5 Section 18 of the Agreement shall apply to this DPA *mutatis mutandis*.

ADDENDUM A

DESCRIPTION OF PROTECTED DATA PROCESSING

Description	Details
Purpose	Provision and receipt, including use, of Services.
Processing activities	For all Customers: ● Support and management of the Customer's business operations on the Services; ● Maintain a directory of Authorized Users; ● Improving user experience and fostering of the adoption and design features that fit user needs relating to the Services; ● Monitoring for metrics, traces and logs to perform LumApps support and security duties; ● Storage. In addition, only for Customers using Journeys as part of the Services: ● Recording, organizing, structuring, adapting or modifying, retrieving, consulting, using, communicating by transmission, disseminating or otherwise making available, matching or linking.
Duration of the processing	The Term of the Agreement and three (3) months thereafter to enable the Customer to retrieve Protected Data.
Categories of personal data	Name, address, title, telephone number, e-mail address, IP address, usernames, and any other Protected Data voluntarily uploaded by the Authorized Users to the Application (for example: job location, date of birth, HR registration number, etc).
Categories of data subjects	Authorized Users as described in the Agreement.

ADDENDUM B:

SECURITY MEASURES

1. Access control to premises and facilities

LumApps implements security measures to prevent unauthorized physical access to premises and facilities holding personal data. These measures include:

- access control system;
- ID reader, magnetic card, chip card;
- door locking (electric door openers, with keys, etc.);
- logging of facility exits/entries;

2. Access control to systems

LumApps restricts unauthorized access to its IT systems to employees with a defined need-to-know or a role requiring such access. These measures include:

- password procedures;
- central management of system access;
- approval procedures for access to IT systems;
- quarterly review of accesses ;

3. Access control to data

LumApps implements security measures to prevent Authorized Users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal, modification or disclosure of data. These measures include:

- granular access rights;
- automated log of user access via IT systems;
- measures to prevent the use of unauthorized automated data-processing systems;
- access must be reviewed every quarter;
- no Customer data will be used in development or test environment;

4. Disclosure control

LumApps implements security measures to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures include:

- compulsory use of a wholly-owned private network for all data transfers;
- encryption using a VPN for remote access, transport and communication of data on unsecure networks;
- prohibition of portable media;
- creating an audit trail of all data transfers;
- AES-256 encryption for data at rest;
- HTTPS TLSv1.2 min data encryption for data in transit;

5. Input control

LumApps implements security measures to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained. These measures include:

- Logging user activities on IT systems;

- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment;
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

7. <u>Availability control</u>

LumApps implements security measures to ensure that data are protected against accidental destruction or loss. These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored;
- Ensure systems are functioning, and that faults are reported;
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system;
- Uninterruptible power supply (UPS);
- Business Continuity procedures;
- Remote storage;
- Antivirus/firewall systems;

8. <u>Segregation control</u>

LumApps implements security measures to allow data collected for different purposes to be processed separately. These measures must include:

- Segregation of business IT systems;
- Restriction of access to data stored for different purposes according to staff duties;
- Segregation of IT testing and production environments;

ADDENDUM C

EUROPEAN ECONOMIC AREA ADDENDUM

1. DEFINITIONS

In this addendum:

"**EEA**" means the European Economic Area;

"**European Data Protection Law**" means the GDPR and any other laws or regulation that are similar, equivalent to, or successors thereto;

"**Model Clauses**" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Protected Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

All capitalized terms and expressions used but not defined in this addendum will have the meaning assigned to them in the applicable European Data Protection Law. For the purpose of this addendum, all references to Applicable Laws shall be read in the context of applicable EU or member state law.

2. INTERNATIONAL TRANSFERS

2.1 To the extent that LumApps processes any Protected Data from the EEA and transfers such Protected Data outside of the EEA to countries not deemed by the European Commission to provide an adequate level of data protection, the parties agree to enter into and comply with the Model Clauses as discussed in Section 3 of this Addendum.

2.2 The parties agree that the data export solution identified in Section 3.1 (Model Clauses) will not apply if and to the extent that LumApps adopts an alternative data export solution for the lawful transfer of Protected Data (as recognized under European Data Protection Law) outside of the EEA. To the extent the execution of additional documents is required to give effect to such data export solution, the Parties shall act reasonably to execute such documentation.

3. MODEL CLAUSES

3.1 Module Two of the Model Clauses are incorporated by reference into this Addendum. Module Two (Controller to Processor) will apply in those instances where Customer acts as a Data Controller and LumApps acts as a Data Processor. Signatures applied to the Agreement(s) will be taken as equally signing and effectuating the Model Clauses.

3.2 In respect to Clause 9(a) (Sub-processors) of Module Two of the Model Clauses, the Parties agree that Option 2 shall apply and the time period will be 30 days.

3.3 In respect to Clause 17 (Governing Law) of Module Two of the Model Clauses: Option 1 is selected, and the governing law is that of France.

3.4 In respect to Clause 18 (Choice of forum and jurisdiction) of Module Two of the Model Clauses: The courts of Paris (France) shall resolve any disputes arising from the Model Clauses.

ANNEX I TO ADDENDUM C

1. LIST OF PARTIES

The data exporter is the Customer. The data importer is LumApps, as defined in the Agreement(s).

2. DESCRIPTION OF PROCESSING/TRANSFER

Data Subjects

2.1 The Protected Data transferred will concern Users as described in the applicable Agreement which may relate to the following categories of Data Subjects: employees, contractors, consultants, individuals belonging to Customer, Customer clients' and partners' workforce and/or other individuals whose Protected Data is Processed as part of the provision of the Services.

Protected Data

2.2 Customer may disclose Protected Data to LumApps which may include, but is not limited to, the following types of Protected Data: identification and contact data (e.g., name, address, phone number, title, email, other contact details); employment details (e.g., job title, role, manager); IT information (e.g., entitlements, IP addresses, usage data, cookies data, online identifiers); domain and device information (e.g., MAC address, hostnames, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), and qualified hostnames); information contained in logs related to security events identified and captured by Services; and/or unstructured data provided to Customer for the purpose of providing support services (e.g., packet capture (PCAP) for file testing).

Sensitive personal data transferred

2.3 The Customer shall not transfer any sensitive personal data (as specified in the Applicable Laws) to LumApps. In the event that such sensitive personal data is transferred and LumApps becomes aware of such transfer, LumApps shall promptly delete such sensitive personal data

Frequency of transfer

2.4 The transfer of Protected Data between the Parties will occur on a continuous basis.

Nature of the Processing:

2.5 Protected Data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available Protected Data.

Purpose

2.6 The purpose of the Processing of Protected Data under this DPA is to enable LumApps to deliver the Services and perform its obligations as set forth in the Agreement(s) (including this DPA) or as otherwise agreed by the Parties in mutually executed written form.

Retention

2.7 The transfer of Protected Data between the parties to facilitate LumApps' Processing on behalf of Customer will occur as needed on an ongoing basis until the termination of the Agreement(s).

Sub-processors

2.8 Please refer to:

https://www.lumapps.com/legal/lumapps-platform-subprocessors/.

3. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Commission Nationale de l'Informatique et des Libertés (CNIL), the data protection authority of France.

ANNEX II TO ADDENDUM C

Description of the technical and organizational measures implemented by the data importer(s)

The technical and organizational measures to be implemented and maintained by LumApps are as described in Section 5 to the DPA. LumApps shall procure that each Authorized Sub-processor implements and maintains, at a minimum, the technical and organizational measures that LumApps is required to implement under the DPA.

ADDENDUM D

UNITED KINGDOM ADDENDUM

1. Definitions

In this addendum:

"**Mandatory Clauses**" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s199A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

"**Model Clauses**" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Protected Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**UK**" means the United Kingdom.

"**UK Data Protection Law**" means all laws relating to data protection, the Processing of Protected Data, privacy and/or electronic communications in force from time to time in the UK, including: (i) the UK GDPR and UK Data Protection Act 2018; and/or (ii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) above.

"**UK GDPR**" as defined in section 3 of the Data Protection Act 2018.

All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law. For the purpose of this addendum, all references to Applicable Laws shall be read in the context of UK law.

2. International Transfers

2.1 To the extent that LumApps Processes any Protected Data from the UK and transfers such Protected Data outside of the UK to countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the Parties agree to enter into and comply with the Model Clauses (as amended by the Mandatory Clauses).

2.2 The Parties agree that the Mandatory Clauses will not apply if and to the extent that LumApps adopts an available, alternative data export solution for the lawful transfer of Protected Data (as recognized under UK Data Protection Law) outside of the UK. To the extent the execution of additional documents is required to give effect to such data export solution, the Parties will work in good faith to execute such documentation.

3. Mandatory Clauses

3.1 The Mandatory Clauses are incorporated by reference into this Addendum and the Model Clauses are amended in accordance with the Mandatory Clauses. Annexes I and II of Addendum C to this DPA (European Economic Addendum) are also incorporated by reference to this Addendum.

3.2 Neither the Mandatory Clauses or this Addendum shall be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.

3.3 For the purposes of this Addendum: the competent supervisory authority shall be the Information Commissioner's Office.

3.4 In respect to Clause 17 *Governing Law*: the governing law is that of England and Wales.

3.5 In respect to Clause 18 *Choice of forum and jurisdiction*: The courts of England and Wales shall resolve any disputes arising from the Model Clauses (as amended by the Mandatory Clauses).

ADDENDUM E

CALIFORNIA CONSUMER PRIVACY ACT ADDENDUM

1. Definitions

All terms used in this addendum and not defined in the DPA or this addendum have the meaning assigned to them in the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act (together, the **"CPRA"**).

2. LumApps' obligations

2.1. LumApps will comply with the CPRA as a **"service provider"** (as defined by the CPRA) in its performance of the Services.

2.2. LumApps shall not: (i) sell or share personal information; (ii) retain, use, or disclose personal information for any purpose other than for the business purposes specified in the Agreement(s), including retaining, using, or disclosing personal information for a commercial purpose other than the business purposes specified in the Agreement(s), or as otherwise permitted by the CPRA; (iii) retain, use, or disclose personal information outside of the direct business relationship between Customer and LumApps; (iv) combine personal information with personal information that LumApps receives from or on behalf of another person or persons or collects from its own interaction with the Data Subject; provided that LumApps may combine personal information to perform any business purpose as defined in regulations adopted pursuant to the CPRA.