Data Processing Agreement (UK & Ireland)

1. Background

1.1 This DPA (the "**DPA**") is executed by and between you ("**Client**") and the LEAP legal entity ("**LEAP**") that is a party to the General Terms governing the provision of the LEAP platform and LEAP products (the "**Agreement**").

1.2 LEAP and the Client are referred to herein, individually, as a "**Party**", and collectively as the "**Parties**".

1.3 This DPA is effective as of the effective date of the Agreement ("**Effective Date**").

1.4 This DPA governs all Processing of Client Personal Data under the Agreement.

2. Definitions

Unless otherwise defined in the Terms or in applicable Data Protection Law (as defined below), the capitalised terms listed in this DPA have the following meanings:

"Affiliate" means any entity that Controls or is under common Control with a Party.

"**Control**" means direct or indirect ownership or control of fifty percent (50%) or more of the voting interests of an entity.

"**Controller**" means the natural or legal person, public authority, agency, or other body which alone or jointly with others, determines the purposes and means of processing Client Personal Data under the Agreement.

"**Client Personal Data"** means any Personal Data processed by LEAP in its capacity as a processor on the Client's behalf in connection with the Client's use of the Services.

"Data Protection Law" means all applicable laws and regulations relating to the processing of Personal Data including:

(a) the UK GDPR;

(b) the GDPR;

(c) Directive 2002/58/EC (ePrivacy Directive);

(d) the Privacy and Electronic Communications (EC Directive) Regulations 2003;

(e) the UK Data Protection Act 2018;

(f) any laws which implement or supplement any such laws; and

(g) any laws which replace, extend, re-enact, consolidate or amend any of the foregoing.

"Data Subject" means an identified or identifiable natural person to whom specific Personal Data relates.

"**De-Identified Data**" means data that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a specific Data Subject.

"GDPR" means, as applicable to either Party or the Services from time to time the General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).

"**Personal Data Breach**" means a breach of LEAP's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data.

"**Processor**" means a natural or legal person, public authority, agency, or body that processes Client Personal Data on behalf of a Controller under the Agreement.

"**Processing**" means any operation performed on Client Personal Data, such as collection, use, storage, disclosure, analysis, deletion, or modification, whether by manual or automated means.

"**Special Category Personal Data**" means Personal Data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; or trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation.

"**Services**" means the products or services that LEAP has agreed to provide pursuant to the Agreement which involve processing of Client Personal Data.

"**Sub-processor**" means any natural or legal person, public authority, agency, or body with whom LEAP contracts to process Client Personal Data.

"**Supervisory Authority**" means an independent public authority established by an EU/EEA member state or other relevant state under Data Protection Law, responsible for monitoring and enforcing the application of Data Protection Law within that jurisdiction.

"Valid Transfer Mechanism" means a mechanism to protect Personal Data that is recognised by the UK government and/or European Commission (as applicable) as providing adequate safeguards for Protected Data transferred outside the UK and/or EEA

3. Roles

3.1 This DPA applies when Client Personal Data is Processed by LEAP.

3.2 In this context, LEAP shall act as processor of Client Personal Data, for which the Client acts as Controller.

3.3 Each Party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including applicable Data Protection Law.

3.4 The Parties agree that this DPA and the Agreement (including the Client providing instructions through the use of LEAP's Services) constitute the Client's documented instructions regarding LEAP's processing of Client Personal Data ("**Written Instructions**").

3.5 For the purposes of this DPA, any Client Personal Data provided to LEAP or LEAP's Affiliates by a Client Affiliate for processing on Client's and/or Client's Affiliate's behalf shall be deemed to be Client Personal Data and to have been provided by Client. The Client represents that it will take all measures reasonably necessary to ensure its Affiliates comply with all Client obligations with respect to this DPA. The Client is responsible for its Affiliates' compliance with all terms of this DPA.

4. Client's Obligations as Controller

4.1 The Client warrants and represents, as Controller, that:

(i) Client Personal Data has been lawfully obtained;

(ii) it has a valid legal basis for processing of Client Personal Data;

(iii) LEAP's receipt, possession or use of Client Personal Data in accordance with this DPA will not place LEAP in breach of any applicable Data Protection Law or infringe any third party rights;

(iv) all data subjects to which Client Personal Data relates are provided with a copy of the Client's privacy policy in accordance with Data Protection Law;

(v) it has appointed a data protection officer at all times for the duration of the Agreement; and

(vi) it shall implement appropriate technical and organisational measures to ensure an appropriate level of security to protect any Client Personal Data.

4.2 The Client shall fully indemnify LEAP in respect of any loss, penalty, fines, costs or expenses howsoever suffered or incurred arising directly or indirectly as a result of:

(i) the Client's failure to comply with its obligations under this DPA; or

(ii) the Client's breach of Data Protection Law.

5. Details of Data Processing

5.1 **Subject matter**: Client Personal Data.

5.2 **Duration:** processing of Client Personal Data commences on the Client's provision of Client Personal Data to LEAP and continues for the duration of the Agreement.

5.3 **Purpose**: the provision of the Services initiated by the Client from time to time.

5.4 **Nature of the processing:** collecting, sorting, storing, transferring, restricting and deleting Client Personal Data.

5.5 **Type of Client Personal Data:** Client Personal Data entered by the Client in the process of using the Services and which may include:

(i) identity data (first name, maiden name, last name, username or similar identifier, title, and date of birth);

(ii) contact data (billing address, delivery address, email address and telephone numbers);

(ii) bank account and payment card details;

(iv) ID document and other personal details such as electronic signatures;

(v) geolocation, IP address, unique device identifiers, device attributes such as operating system/browser type; and

(vi) biometric data including facial recognition for login purposes, voice recordings and facial images.

5.6 **Categories of data subjects:** Client's clients, employees, staf, personnel, and suppliers.

6. LEAP's Obligations as Processor

6.1 In LEAP's capacity as Processor, LEAP shall:

(a) only process the Client Personal Data to the extent, and in such a manner, in accordance with the Client's Written Instructions;

(b) promptly notify the Client if, in its opinion, the Client's Written Instructions do not comply with Data Protection Law;

(c) maintain the confidentiality of the Personal Data and not disclose the Personal Data to third parties unless it is necessary to maintain or provide the Services, specifically authorised by the Client or this DPA, or as required by domestic law, court or regulator. If a domestic law, court or regulator (including the Supervisory Authority) requires LEAP to process or disclose the Client

Personal Data to a third party, LEAP shall (to the extent permitted by law) give the Client reasonable notice of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement; and

(d) reasonably assist the Client, at the Client's cost, with meeting the Client's compliance obligations under Data Protection Law, taking into account the nature of LEAP's processing and the information available to LEAP, including in relation to Data Subject rights, data protection impact assessments, and reporting to and consulting with the Supervisory Authority under Data Protection Law. If a Data Subject makes a request to LEAP, LEAP shall promptly forward the request to the Client once LEAP has identified that the request is from a Data Subject for whom the Client is responsible. The Client authorises LEAP to respond to a Data Subject who makes a request to LEAP, to confirm that LEAP has forwarded the request to the Client. The Client is solely responsible for responding to any Data Subject request.

6.2 **LEAP's Employees**

6.2.1 LEAP shall ensure that all of its employees are informed of the confidential nature of the Client Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Client Personal Data.

6.3 **Security**

6.3.1 LEAP shall at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Client Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Client Personal Data.

6.3.2 LEAP shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of Client Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Client Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6.4 **Sub-processors**

6.4.1 The Client hereby expressly consents to, and provides its general authorisation for, LEAP to engage Sub-processors to process Client Personal Data, subject to clause 6.4.6.

6.4.2 LEAP's current list of all Sub-processors it engages to process Client Personal Data are set out

in the relevant Sub-processor list identified at https://www.leaplegalsoftware.com/legal/sub-processors.

6.4.3 Subject to clause 6.4.4 of this DPA, at least 30 days before LEAP engages a new Sub-processor, LEAP shall update its Sub-processor list and notify the Client of such update.

6.4.4 LEAP shall notify the Client without undue delay following the appointment of a new Sub-processor if immediate appointment is required to maintain the security of Client Personal Data or to comply with Data Protection Law or applicable law.

6.4.5 If the Client reasonably objects to a new Sub-processor, the Client can:

(a) not place further orders for the relevant LEAP Products;

(b) cease using the LEAP Product for which LEAP has engaged the Sub-Processor; or

(c) notify LEAP in writing within thirty (30) days after the Sub-processor's appointment. In LEAP's sole discretion, LEAP may use reasonable efforts to address the Client's objection. If the Parties are unable to resolve the Client's objection within thirty (30) days, the Client may terminate this DPA and any portion of the Agreement relating to the processing of Client Personal Data.

6.4.6 If the Client does not object to a new Sub-processor within thirty (30) days of LEAP's notice of the Sub-processor's appointment, the Client will be deemed to have accepted the new Sub-processor.

6.4.7 Where LEAP engages a Sub-processor, LEAP shall:

(a) enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by LEAP under this DPA, such written agreement shall be at least as protective of Client Personal Data as this DPA; and

(b) LEAP shall remain liable for its Sub-processors' acts and omissions that cause LEAP to breach any of LEAP's obligations under this DPA.

6.5 **Personal Data Breach**

6.5.1 LEAP shall without undue delay notify the Client if it becomes aware of any Personal Data Breach.

6.5.2 Where LEAP becomes aware of a Personal Data Breach, it shall, without undue delay, also provide the Client with the following information:

(c) a description of the nature of the Personal Data Breach, including the categories of Client Personal Data and the approximate number of both Data Subjects and the Personal Data records concerned;

(d) the likely consequences of the Personal Data Breach; and

(e) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

6.5.3 The Client shall determine:

(a) whether to provide notice of accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Supervisory Authority, other relevant regulators, law enforcement agencies or others, as required by law or regulation or in the Client's discretion, including the contents and delivery method of the notice. If and to the extent LEAP is referenced by name in any such communication, LEAP shall be provided with an opportunity to review and approve the communication for accuracy, such approval not to be unreasonably withheld; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.5.4 LEAP's acknowledgement of a Personal Data Breach or decision to notify the Client of a Personal Data Breach is not an admission of fault or liability.

7. Audits

7.1 LEAP shall, at the Client's written request, permit and contribute to audits and inspections of LEAP's processing activities relating to Client Personal Data. Such audits may be conducted by the Client or by an independent third-party auditor mandated in writing by the Client, provided that:

(a) the Client gives LEAP no less than 60 Business Days' prior written notice, except where a Supervisory Authority requires a shorter period or where the Client has reasonable grounds to suspect a material breach;

(b) audits are conducted during normal business hours in a manner that minimises disruption to LEAP's operations;

(c) the LEAP systems, premises or documentation accessed during the course of the audit constitute confidential information under the terms of the Agreement;

(d) any Client mandated auditor executes a confidentiality undertaking in a form reasonably acceptable to LEAP before accessing any LEAP systems, premises, or documentation;

(e) the Client bears its own costs and the reasonable costs of LEAP's cooperation, unless the audit reveals a material non-compliance by LEAP, in which case LEAP shall bear its own costs; and

(f) no more than one audit is conducted per calendar year, except where required by a Supervisory Authority.

7.2 As an alternative to an audit under clause 7.1, LEAP may, at its discretion, satisfy the Client's audit request by providing the Client with relevant summaries and/or redacted copies of a third-party audit

report, certification, or security attestation (such as ISO 27001 or equivalent) covering the relevant processing activities of Client Personal Data, provided that such report or certification is no more than 12 months old. The Client may only require an audit under clause 7.1 where such documentation does not reasonably address the Client's specific compliance concerns.

8. Return or Deletion of Client Personal Data

8.1 At the Client's written direction, LEAP shall delete, return or anonymise Client Personal Data and copies thereof to the Client as soon as reasonably practicable on termination of the Agreement, except for copies that LEAP may retain for audit or archiving purposes, or unless otherwise required by Data Protection Law to store Client Personal Data.

9. Termination

9.1 Unless terminated earlier pursuant to the Agreement or any other applicable provision of this DPA or any applicable Data Protection Laws, this DPA shall terminate upon the completion of Processing or termination of the Agreement, whichever is later.

10. International Transfers of Personal Data

10.1 LEAP's processing of Client Personal Data may involve Processing regulated by one or more Data Protection Laws and/or may involve the international transfer of Client Personal Data.

10.2 The Client hereby authorises LEAP to transfer Client Personal Data for the purposes referred to in clause 5.3 to recipients outside of the United Kingdom and/or EEA ("**International Recipients**") provided that:

(a) LEAP takes all necessary steps to ensure that transfers of Protected Data outside the United Kingdom and/or EEA are effected by way of Valid Transfer Mechanisms;

(b) LEAP shall document the Valid Transfer Mechanism relied upon in each transfer of Client Personal Data;

(c) if the transfer mechanism relied upon becomes invalid or if the International Recipient is not able to comply with the requirements of the transfer mechanism or the obligations set out in the data transfer clauses due to local laws or for any other reason, LEAP shall either put in place an alternative Valid Transfer Mechanism or immediately cease the relevant data transfers().

10.3 The provisions of this Agreement shall constitute the Client's instructions with respect to transfers of the Protected Data for the purpose of this Agreement.

11. General

11.1 This DPA constitutes the entire agreement between the Parties concerning the subject matter of this DPA and supersedes all prior or contemporaneous representations, understandings, agreements, and communications between the Parties, whether written or verbal, regarding the subject matter of this DPA.

11.2 In the event of a conflict between this DPA and the Agreement (or any other agreement between the Parties), this DPA will govern and control with respect to the subject matter of this DPA.

11.3 This DPA may be modified or amended by LEAP in its sole discretion. If the Client disagrees with such amendment, the Client's sole remedy is to terminate that portion of the Agreement relating to the Processing of Client Personal Data on thirty (30) days' notice. Unless expressly agreed by the Parties in writing, any amendment of this Agreement is effective only with respect to Processing that occurs after the date of such amendment.

11.4 If any provision of this DPA is found to be unenforceable, then that provision shall be modified to the extent necessary to make it enforceable and the remainder of this DPA shall remain in effect.

12. Governing Law and Jurisdiction

12.1 This DPA is governed by the laws stipulated in the Agreement, except to the extent otherwise required by the Data Protection Laws, in which case the laws of the jurisdiction prescribed by the Data Protection Laws apply. No provision of this DPA shall be deemed to limit any person's rights or obligations under any applicable Data Protection Laws.