Cledara Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to the 'SERVICES TERMS AND CONDITIONS' or other written or electronic agreement between Customer and Cledara Ltd. ("**Cledara**") for the provision of Services to Customer ("**Agreement**") and applies where, and to the extent that, Cledara processes Customer Data (defined below) on behalf of Customer when providing Services under the Agreement. All capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where otherwise indicated, the term "**Customer**" shall include the Customer and its Controller Affiliates.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**CCPA**" means the California Consumer Protection Act of 2018, upon the effective date thereof and as may be amended from time to time.

"**Customer Data**" means any personal data that Cledara processes on behalf of Customer in the course of providing Services, and includes "personal information" as defined in the CCPA.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

"**Controller Affiliates**" means any of Customer's Affiliate(s): (a) (i) that are subject to Data Protection Laws of the EEA, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Cledara, but have not signed their own ordering document and are not a "Customer" as defined under the Agreement, (b) if and to the extent Cledara processes Customer Data for which such Affiliate(s) qualify as the controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to a party and its processing of Personal Data under the Agreement, including, where applicable, GDPR (or in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data protection and privacy as a consequence of the United Kingdom leaving the European Union); in each case, as may be amended, superseded or replaced.

"**EEA**" means for the purposes of this DPA the European Economic Area, United Kingdom and Switserland.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"**Model Clauses**" means the Standard Contractual Clauses (Processors) (2010/87/EU): Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), which do not ensure an adequate level of data protection.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification programs operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016, and by the Swiss Federal Council respectively (as may be amended, superseded or replaced).

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Security Incident**" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Data.

"**Services**" means the generally available Cledara product or service provided by Cledara to Customer pursuant to the Agreement.

"**Sub-processor**" means any Processor having access to Customer Data and engaged by Cledara to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Cledara Affiliates but shall exclude any employee, consultant or contractor of Cledara.

"**controller**", " **processor**", "**processing**" and "**personal data**" shall have the meanings given to them in the GDPR.

2. Roles and Scope of Processing

2.1 Scope of this DPA. This DPA applies where and only to the extent that Cledara processes Customer Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement.

2.2 Role of the Parties. As between Cledara and Customer, Customer is the data controller of Customer Data and Cledara shall process Customer Data only as a data

processor acting on behalf of Customer and, with respect to the CCPA, as a "service provider" as defined therein. Cledara will only process Customer Data for the following purposes: (i) processing to perform any steps necessary for the performance of the Agreement; (ii) processing to provide the Services in accordance with the Agreement; (iii) processing initiated by end users in their use of Services; (iv) processing required in order to meet obligations arising from financial regulation and/or associated legislation and (v) processing to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of this DPA (individually and collectively, the "Purpose") and only in accordance with Customer's documented lawful instructions.

2.3 Processing Instructions. The parties agree that (i) the Agreement (including this DPA) sets out Customer's complete and final instructions to Cledara for the processing of Customer Data; and (ii) processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Cledara. Customer shall ensure its instructions are lawful and that the processing of Customer Data in accordance with such instructions will not violate applicable Data Protection Laws.

2.4 Details of Data Processing

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between Cledara and Customer, the duration of the data processing under this DPA is the term of the Agreement, or longer, if required by Cledara to comply with obligations arising from financial regulation and/or associated legislation.

(c) Purpose: Cledara shall process Customer Data only for the Purpose.

(d) Nature of the processing: Cledara performs SaaS purchasing and management capabilities, and such other services, as more particularly described in the Agreement.

(e) Categories of data subjects: vendors; Customer's end-users (past, potential, present and future) authorised to use the Services, Customer's shareholders (past, present and future) and Customer's directors (past, present and future)

(f) Types of Customer Data: The types of Customer Data may include name, title, address, phone number, email address, date of birth and other personal data subject to the conditions of the Agreement, including Customer data contained in any passport and proof of address, or other similar documents provided by the Customer.

2.5 Customer Processing of Customer Data. Customer agrees that it: (i) will comply with its obligations under Data Protection Laws in respect of its processing of

Customer Data; and (ii) has provided notice and obtained (or will obtain) all consents and rights necessary for Cledara to process Customer Data pursuant to the Agreement and this DPA.

3. Subprocessing

3.1 Sub-processor Obligations. Where Cledara authorises any Sub-processor:

(a) Customer acknowledges and agrees that (a) Cledara's Affiliates may be retained as Sub-processors through written agreement with Cledara and (b) Cledara and Cledara's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Personal Data, Cledara or an Cledara Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor.

(b) A current list of Subprocessors for the Services including the identities of those Sub-processors and their country of location, shall be made on written request by the Customer; Customer is to email by e-mailing dpo@cledara.com if it requires this information. A Customer can request to subscribe to, and Cledara shall provide, notifications of new Sub-processor(s) before authorising such new Sub-processor(s) to process Customer Data in connection with the provision of the applicable Agreement, such notification shall be communicated via email to the email that subscribes.

(c) Customer may reasonably object to Cledara's use of a new Sub-processor (e.g., if making Customer Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Customer Data) by notifying Annotate promptly in writing within ten (10) business days after receipt of Cledara's notice in accordance with the mechanism set out in Section 4.2. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Cledara will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Cledara is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Agreement(s) with respect only to those Services which cannot be provided by Cledara without the use of the objected-to new Sub-processor by providing written notice to Cledara. Cledara will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of

termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

4. Security Measures and Security Incident Response

4.1 Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

5. Audits

5.1 Customer Audits. Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Cledara to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Cledara written notice as provided for in the Agreement. If Cledara declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

6. International Transfers

6.1 Location of Processing. Cledara may transfer (directly or via onward transfer) and process Customer Data anywhere in the world where Cledara or its Sub-processors maintain data processing operations, provided that Cledara will at all times ensure that such transfers are done in compliance with the requirements of applicable Data Protection Laws and this Section 6.

6.2 Data Transfers. To the extent that Cledara is a recipient of any Customer Data under the Agreement that is protected by Data Protection Laws applicable to the EEA, and such Customer Data is being transferred to a country that does not provide an adequate level of protection under applicable Data Protection Laws, the parties agree that Cledara shall provide an adequate protection and/or appropriate safeguards for such Customer Data by complying with the Standard Contractual Clauses. In the event

the Privacy Shield does not apply to the transfer, is not accepted as a valid transfer mechanism under Data Protection Laws, is invalidated and/or Cledara is no longer certified under Privacy Shield, Cledara agrees to abide by and process the Customer Data in compliance with the Model Clauses, which are incorporated by reference and form an integral part of this DPA. For the purposes of the Model Clauses, the parties agree that Cledara is a "data importer" and Customer is the "data exporter" (notwithstanding that the Customer may be an entity located outside the EEA.

7. Return or Deletion of Data

7.1 Upon termination or expiration of the Agreement, Cledara shall delete all Customer Data in its possession or control. This requirement shall not apply to the extent Cledara is required by applicable law or financial regulation to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Cledara shall securely isolate and protect from any further processing, except to the extent required by law or regulation.

8. Cooperation

8.1 To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Cledara shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer in responding to any requests from individuals or applicable data protection authorities relating to the processing of personal data under the Agreement. In the event that any such request is made to Cledara directly, Cledara shall not respond to such communication directly without Customer's prior authorisation, unless legally compelled to do so. If Cledara is required to respond to such a request, Cledara will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 If a law enforcement agency or regulatory authority sends Cledara a demand for Customer Data (for example, through a subpoena or court order), Cledara will attempt to redirect the law enforcement agency or regulatory authority to request that Customer Data directly from Customer. As part of this effort, Cledara may provide Customer’s basic contact information to the law enforcement agency or regulatory authority. If compelled to disclose Customer Data to a law enforcement agency or regulatory authority, then Cledara will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Cledara is prohibited from doing so by law or regulation.

8.3 To the extent Cledara is required under Data Protection Laws applicable to the EEA, Cledara will provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

9. Controller Affiliates

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between Cledara and each such Controller Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10 below. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Customer.

9.2 Communication. The Customer entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Cledara under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

9.3 Rights of Controller Affiliates. If a Controller Affiliate becomes a party to the DPA with Cledara, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against Cledara directly by itself, in which case the parties agree that: (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together.

10. Limitation of Liability

10.1 Any claim or remedies the Customer or a Controller Affiliate may have against Cledara and its respective employees, agents and Sub-processors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under GDPR, including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under the Privacy Shield and/or Model Clauses (as applicable), will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement.

10.2 For the avoidance of doubt, Cledara and its Affiliates' total liability for all claims from the Customer and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Controller Affiliate that is a contractual party to any such DPA.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. General

11.1 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

11.2 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.3 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

11.4 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer, as defined this Data Processing Addendum (the "data exporter")

And

Cledara Limited, 3rd Floor 86-90 Paul Street, London, England, EC2A 4NE (the "data importer")

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the

processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Defined terms used in this Appendix 1 shall have the meaning given to them in the Agreement (including the DPA).

Data exporter

The data exporter is the legal entity specified as “Customer” in the DPA.

Data importer

The data importer Cledara Limited.

Data subjects

Please see Section 2.4 of the DPA, which described the data subjects.

Categories of data

Please see Section 2.4 of the DPA, which described the categories of data.

Processing operations

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or
2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorised Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorisation: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

ii) Preventing Unauthorised Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer accounts and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Penetration testing: We maintain relationships with industry recognised penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorisation Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents, maintain regulatory compliance and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged.

Background checks: All Cledara employees undergo a background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All Cledara employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer account at Cledara. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimise product and Customer damage or unauthorised disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability sones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.