Cledara Customer Data Processing Addendum

Effective Date: 23 February 2022

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 annexed to the European Commission's Implementing decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**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, which 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.

Unless such transfer is otherwise permitted under EU Data Protection Law, transfers to a subprocessor in any country not recognized under EU Data Protection Law as providing an adequate level of protection for Your Controlled Data shall proceed pursuant to (a) the processor to processor (module 3) standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR and approved by the European Commission decision 2021/914, dated 4 June 2021; or (b) such other standard contractual clauses for the transfer of personal data to third countries that are recognised under the applicable EU Data Protection Law in the EEA, UK or Switzerland.

Any European Commission standard contractual clauses between you and Cledara Limited in respect of Your Controlled Data that were put in place pursuant to a previous version of this DPA are terminated with effect from 23 February 2022. You agree that Your Controlled Data transferred pursuant to the terminated standard contractual clauses shall not be destroyed or returned due to such termination, but instead, shall continue to be processed in accordance with and subject to the terms of this DPA and as if transferred pursuant to the standard contractual clauses identified in Section 6.2.

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 Model Clauses, 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

SECTION I

Clause 1

Purpose and scope

The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

The Parties:

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"). These Clauses apply with respect to the transfer of personal data as specified in the Data Processing Addendum. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

   iii) Clause 9(a), (c), (d) and (e);

   iv) Clause 12(a), (d) and (f);

   v) Clause 13;

   vi) Clause 15.1(c), (d) and (e);

   vii) Clause 16(e);

   viii) Clause 18(a) and (b).

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in the Data Processing Addendum.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in the Data Processing Addendum., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in the Data Processing Addendum. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Data Processing Addendum.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    ii) refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability

Clause 13

Supervision

a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards

   iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

d) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

e) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

f) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

    i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

    ii) the data importer is in substantial or persistent breach of these Clauses; or

    iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

    In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

c) The Parties agree to submit themselves to the jurisdiction of such courts.

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 describes the data subjects.

Categories of data

Please see Section 2.4 of the DPA, which describes 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:

Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or

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.