Cledara Customer Data Processing Addendum

Last modified: December 4, 2024

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the 'SERVICES TERMS AND CONDITIONS' or other written or electronic agreement ("**Principal Agreement**") between Customer and Cledara Ltd. of 3rd Floor 86-90 Paul Street, London, England, EC2A 4NE, Company identification number 11455090 ("**Cledara**" or the "**Processor**") for the provision of Services to Customer. This DPA applies where, and to the extent that, Cledara processes Customer Data (defined below) on behalf of Customer when providing Services under the Principal Agreement.

This Agreement governs the specific requirements of Data Protection Laws to the extent that Company's use of Cledara Services implies the processing of Personal Data subject to Data Protection Laws.

This Agreement is complementary to our Privacy Policy, which serves as the primary reference for our data protection practices and measures.

The term of this Agreement shall follow the term of the Principal Agreement. Terms not defined herein shall have the meaning as set forth in the Principal Agreement.

WHEREAS

A The Customer acts as a Data Controller (the "**Controller**");

B The Customer wishes to subcontract certain Services (as defined below), which imply the processing of Personal Data, to Cledara Ltd., acting as a Data Processor (the "**Processor**");

C The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation) and other applicable data protection laws;

D The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation
Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.2 "**Company Personal Data**" means any Personal Data related to the Company or Company's customers or employees Processed in connection with the Principal Agreement;

1.3 "**Contracted Processor**" means a Subprocessor;

1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.5 "**EEA**" means the European Economic Area, United Kingdom and Switzerland;

1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.8 "**Data Transfer**" means:

1.8.1 a transfer of Company Personal Data from Controller to the Processor or a Contracted Processor; or

1.8.2 an onward transfer of Company Personal Data from the Processor to a Subprocessor, or between two establishments of a Subprocessor;

1.9 "**Services**" means SaaS purchasing and management capabilities and other services provided by the Processor, such as software subscription management, payment processing, and other services as developed by the Processor. The details and pricing of the Services can be found on the Processor's website;

1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Agreement;

1.11 "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq, and its implementing regulations;

1.12 "**UK GDPR**" "UK GDPR" means the Data Protection Act 2018 and the GDPR as it forms part of UK law by virtue of the European Union (Withdrawal) Act 2018;

1.13 "**Standard Contractual Clauses**" means:

a) The standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**2021 SCCs**");

b) The UK International Data Transfer Agreement ("**IDTA**") or the UK Addendum to the 2021 SCCs; c) The 2021 SCCs as modified for Switzerland according to FDPIC guidance;

1.14 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.15 **"Sensitive Data**" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation, criminal convictions and offenses, or data relating to children.

The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR or other applicable Data Protection Law, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

Processor shall:

2.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data;

2.2 not process Company Personal Data other than on Controller's documented instructions unless Processing is required by Applicable Laws.

Controller instructs Processor to process Company Personal Data to:

2.3 provide the Services and related technical support;

2.4 process to perform any steps necessary for the performance of the Agreement;

2.5 process to provide the Services in accordance with the Agreement;

2.6 process as initiated by end users in their use of Services;

2.7 process required in order to meet obligations arising from financial regulation and/or associated legislation;

2.8 process to comply with other reasonable instructions provided by Customer that are consistent with the terms of this Agreement.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and/or to comply with Data Protection Laws in the context of that

individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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 implement appropriate technical and organizational 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 The Processor shall also assess the risks associated with processing activities and apply measures that are consistent with the requirements set forth in Article 32(1 GDPR, ensuring the security of Company Personal Data at all times.

5. Subprocessing

5.1 Customer acknowledges and agrees that (a Processor's Affiliates may be retained as Sub-processors through written agreement with Processor and (b Processor and Processor's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

5.2 A current list of Subprocessors for the Services including the identities of those Sub-processors and their country of location, shall be made available to the Customer on written request by emailing dpo@cledara.com or via trust.cledara.com.

5.3 Processor ensures that Subprocessors are subject to an agreement with Processor no less restrictive and protective than the present Agreement with respect to the protection of Company Personal Data to the extent applicable to the nature of the services provided by the Subprocessor.

5.4 Customer may reasonably object to Processor's use of a new Sub-processor by notifying Processor promptly in writing within ten (10 business days after receipt of Processor's notice. In the event Customer objects to a new Sub-processor, Processor will use 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.

6. Data Subject Rights

6.1 Taking into account the nature of the processing, Processor shall reasonably assist Company for the fulfilment of Company's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

a) promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

b) ensure that it does not respond to that request except on the documented instructions of Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 The Processor shall manage any Personal Data Breach in compliance with applicable Data Protection Laws and its internal Personal Data Breach procedures.

7.2 In the event of a Personal Data Breach affecting Company Personal Data, the Processor shall notify the Company without undue delay, providing sufficient information to enable the Company to fulfill its obligations under Data Protection Laws, including informing Data Subjects as necessary.

7.3 Processor shall co-operate with Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

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

10. Audit rights

10.1 Subject to sections 10.2 to 10.4, Processor shall make available to Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by Company or an auditor mandated by Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Customer shall give Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

10.3 A Customer exercising its audit rights under section 10.1 shall give Processor not less than 60 days' prior written notice of its intention to audit. Processor and Customer shall mutually agree on the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible.

10.4 Processor need not give access to its premises for the purposes of such an audit or inspection:

a to any individual unless they produce reasonable evidence of identity and authority;

b outside normal business hours at those premises; or
c for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which Customer is required to carry out under Data Protection Laws or by a Supervisory Authority.

11. CCPA Compliance

11.1 Processor certifies that it:
a) Understands and will comply with CCPA restrictions;
b) Will not sell or share Personal Information;
c) Will process Personal Information only for Business Purposes specified in this DPA;
d) Will notify Customer if it can no longer meet CCPA obligations.

12. International Transfers

12.1 To the extent possible, the Processor shall only transfer or authorize the transfer of Data to countries within the EEA and/or countries subject to an adequacy decision, as provided for in art. 45 GDPR.

12.2 If Personal Data processed under this Agreement is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that the Personal Data are adequately protected.

12.3 Personal Data may be transferred from:

- European Union Member States

- European Economic Area (EEA) countries (Norway, Iceland, Liechtenstein)
- United Kingdom
- Switzerland

to countries that the relevant authority has determined provide adequate protection through:

- European Commission adequacy decisions
- UK adequacy regulations
- Swiss adequacy decisions

12.4 As of December 2024, this includes transfers to:

- Organizations in the United States certified under the EU-US Data Privacy Framework (for EU transfers)
- Organizations in the United States certified under the UK Extension to the EU-US DPF (for UK transfers)
- Organizations in the United States certified under the Swiss-US DPF (for Swiss transfers)

12.5 **Transfers to Other Countries**

12.5.1 For EU/EEA Transfers: Where Personal Data is transferred from the EU/EEA to countries without an adequacy decision, such transfers shall be governed by the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "2021 SCCs").

12.5.2 For UK Transfers: Where Personal Data is transferred from the UK to countries without UK adequacy regulations, such transfers shall be governed by either:

- The International Data Transfer Agreement (IDTA); or
- The 2021 SCCs combined with the UK International Data Transfer Addendum

12.5.3 For Swiss Transfers: Where Personal Data is transferred from Switzerland to countries without Swiss adequacy decisions, such transfers shall be governed by the 2021 SCCs as modified according to the guidance of the Swiss Federal Data Protection and Information Commissioner.

12.6 **Onward Transfers**

12.6.1 Where Processor makes onward transfers to Sub-processors in countries without adequacy decisions:

- For EU/EEA data: The 2021 SCCs (Module Three: Processor to Processor) shall apply
- For UK data: The IDTA or UK Addendum shall apply

- For Swiss data: The modified 2021 SCCs shall apply

12.6.2 Processor shall ensure all onward transfers include appropriate technical and organizational safeguards in addition to the contractual safeguards provided by the transfer mechanisms above.

13. Authorized Affiliates

13.1 Contractual Relationship Customer enters into this DPA on behalf of itself and its Authorized Affiliates. Each Authorized Affiliate agrees to be bound by the obligations under this DPA.

13.2 Communication Customer shall coordinate all communication with Processor under this DPA and be entitled to make and receive communications on behalf of its Authorized Affiliates.

13. General Terms

13.1 Governing Law and Jurisdiction. This Agreement shall be governed by English law, without regard to choice or conflicts of law provisions, and any disputed actions, claims or causes of action arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of England and Wales.

13.2 Severability. 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.

13.3 Amendments. This Agreement may be amended at any time by a written instrument duly signed by both Parties.