Cora Data Protection Appendix

The Power of Perspective

Table of Contents

The parties agree that this Cora Data Protection Appendix (the "**CDPA**") sets forth their obligations with respect to the Processing of Personal Data in connection with the performance of the Subscription Services Agreement ("**SSA**"). This CDPA forms an integral part of the SSA and is effective upon execution of a Sales Order. In case of any conflict, this CDPA will have precedence over the terms of the SSA to the extent of such conflict.

Definitions

"**Applicable Data Protection Law**" means all data protection laws that apply to the Processing Personal Data under this CDPA.

"**Breach**" means a breach of physical or digital security that results in accidental or unlawful destruction, loss, alteration, or disclosure of, or access to, the Personal Data. Unsuccessful attempts or activities that do not compromise the security of Personal Data shall not be considered a Breach, including failed log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Cora**" Means the Cora Systems Affiliate that has executed the SSA.

"**California Personal Data**" Means Personal Data that is subject to the CCPA.

"**CCPA**" means the California Consumer Privacy Act of 2018 (California Civil Code Sec. 1798.100).

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**Data Protection Requirements**" means European Data Protection Laws, and any applicable laws regulations, and other legal requirements relating to privacy, data security, and the use, collection, storage, retention, disclosure, transfer, and processing of Personal Data.

"**Data Subject**" means an identified or identifiable natural person.

"**European Data Protection Laws**" means data laws applicable in the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom. This includes (i) 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) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) UK Data Protection Act 2018 ("**UK DPA**"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("**Swiss DPA**"); in each case, as may be amended, superseded or replaced.

"**European Data**" means Personal Data that is subject to the GDPR.

"**Instructions**" means the written instructions issued by a Controller to a Processor to direct such Processor to perform a specific or general action with respect to Personal Data.

"**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"**Process**" or "**Processing**" is as defined in the Applicable Data Protection Law.

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

"**Standard Contractual Clauses**" means those clauses in the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of data to third countries pursuant to Regulation (EU) 2016/679.

All other capitalized but undefined terms shall have the definitions given them in the SSA.

1 Scope

a)   This CDPA applies to Cora's Processing of Personal Data on behalf of Customer to provide the Services as set forth in the SSA.

b)   The parties acknowledge Customer is the Controller and Cora is the Processor with respect to the Services.

2 Responsibilities of the Parties

a)   Cora shall only process Personal Data in accordance with Instructions from Customer.

b)   Both parties shall, where applicable, comply with transparency and lawfulness requirements under applicable data protection laws including with respect to the rights of Data Subjects.

c)   Customer is responsible for the accuracy, quality and lawfulness of the Customer Data.

d)   In particular, Customer shall ensure any Personal Data has been lawfully collected under an appropriate legal basis and may lawfully be provided to Cora in accordance with the terms of the SSA and this CPDA.

e)   The parties do not contemplate the Processing of Sensitive Personal Data or special categories of Personal Data. Unless otherwise provided in the SSA or Sales Order, Customer may not provide Sensitive Personal Data to Cora.

f)   Customer is responsible for determining whether the security measures provided for the Services meet Customer's obligations under Applicable Data Protection Laws including with respect to the security of data while in transit to and from the SaaS.

g)   Customer recognizes Cora's mobile and web applications are freely accessible to Customer's Users and control over locations from which the app may be accessed lies with the Customer and not with Cora. Customer shall be responsible for authorization and management of User accounts across geographies including with respect to the transfer of Personal Data.

3 Controller Instructions:

a) The parties agree that the Customer's complete Instructions to Cora in relation to the Processing of Personal Data includes the SSA together with Customer's use of the Services in accordance with the SSA.

b) Customer may provide additional reasonable written Instructions during the Subscription Term with respect to the Processing in accordance with Applicable Data Protection Law and Cora shall comply with such instructions to the extent necessary for Cora to (i) comply with its obligations as a Processor or (ii) to assist Customer to comply with its obligations under Applicable Data Protection Law in relation to Customer's use of the Services.

c) As between the Parties, Cora shall have no liability arising from Cora's compliance with instructions received from Customer. However, Cora shall notify Customer where it believes it has received Instructions that are unlawful or beyond the scope of Cora's obligations in operating the Services or providing Professional Services to Customer. The parties acknowledge that Cora is reliant upon Customer's representations regarding the extent to which Cora is entitled to Process the Personal Data.

d) If Cora receives Instructions to Process Personal Data in a way that goes beyond what is covered by the fees for the Services as described in the SSA, Cora shall notify Customer of any additional fees Cora expects to incur in complying with such Instructions and the parties shall negotiate in good faith with respect to any such charges or fees.

4 Confidentiality

Cora shall ensure that persons Cora authorizes to process the Personal Data are under appropriate confidentiality obligations in relation to the Personal Data.

5 Security

Cora shall implement and maintain appropriate technical and organisational safeguards to prevent the accidental or unlawful destruction, loss, alteration, or disclosure of the Personal Data as described in the Security Policy which includes further details on Cora's security measures in relation to the Services specified in the Sales Order. Such measures are designed to maintain the security, confidentiality, and integrity of Customer Data and include physical access controls, redundancy, data separation, and risk assessment and management processes. Notwithstanding any provision to the contrary, Cora may modify or update the Security Policy at Cora's discretion provided such update does not result in a material degradation in protection.

6 Subprocessors

a) Customer confirms Cora may utilize Sub-Processors to Process Personal Data. Cora's Sub-Processors are listed in the Customer Portal and Cora shall notify Customer prior to engaging any additional Sub-Processors where such notice is required by law.

b) Cora shall impose contractual data protection obligations on Sub-Processors that provide at least the same level of protection for Personal Data as does this CDPA. Where appropriate, this shall include Standard Contractual Clauses.

c) Cora shall be responsible for the acts and omissions of each Sub-Processor in relation to such Sub-Processors commitments under Applicable Data Protection Law and in relation to compliance with the commitments in this CDPA.

7 Privacy requests from individuals

a) Customer may address privacy requests received from individuals by utilizing the SaaS functionality or, to the extent such access is not available, Customer may seek assistance from Cora by submitting a support request as outlined in the Service Level and Support Objectives (the "Service Levels") with detailed instructions on how Cora may fulfil such request.

b) If Cora receives requests from individuals for which Customer is the Controller, it shall pass on such requests to Customer whereupon Customer shall become responsible for responding to such request.

c) The parties acknowledge Customer is solely responsible for carrying out its obligations as a Controller. Where applicable, Cora will assist Customer in complying with Customer's obligations as a Controller pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of Processing, by providing information required to conduct Data Protection Impact Assessments or responding to Data Subject access requests. The foregoing is subject to Clause 3d (Controller Instructions).

8 Deletion or Return of Personal Data

Upon termination or expiration of the SSA, Cora shall return, including by providing available data retrieval functionality, or delete any remaining copies of the Customer Data (including Personal Data) Processed under this CDPA in accordance with the procedures set out in the Service Levels. This Clause 8 shall apply except to the extent Cora is required by applicable law to retain data, records, or information.

9 Audits

a) Cora will, upon reasonable request and to a maximum of once per year, provide Customer with sufficient information to enable the Customer to ensure Cora complies with its obligations under this CDPA.

b) Subject to Clause 9d, Customer may itself audit Cora's compliance with its commitments under this CDPA once per year. Additionally, to the extent required by Applicable Data Protection Law, Customer or a competent regulatory authority may perform more frequent audits.

c) Subject to Clause 9b and Clause 9d, Customer may, at its own cost, appoint an independent auditor for the purposes of exercising its rights under this Clause 9 (Audits) subject to Cora's reasonable written agreement to Customer's choice of third-party auditor.

d) For any audit Customer wishes to perform whether itself or through a third party, Customer shall;

    a. Submit an audit plan to Cora two weeks in advance of the proposed audit date describing the scope, duration, and date of the audit.

    b. Cora shall review such plan, notify Customer if it has any questions or concerns, and cooperate with Customer to agree on a final audit plan.

    c. Compensate Cora for reasonable costs Cora incurs as a result of the audit.

e) Any audit shall be conducted during regular business hours.

f) Any auditor shall be under appropriate contractual or statutory confidentiality obligations and all information relating to such audit shall be subject to the Confidentiality provisions of the SSA. Audit reports may only be used to confirm Cora's compliance with the requirements of this CDPA or meeting Customer's own regulatory audit requirements. Cora shall have the right to review audit reports and to issue a reply prior to issuance of a final version. The Customer shall ensure the requirements of this Clause 9f are present in Customer's contract with any third-party auditor.

10 Data Transfers

a) Customer acknowledges and agrees that, without prejudice to any applicable restrictions specified in Customer's Sales Order or the Agreement, Cora may Process Personal Data globally as necessary to perform the Services. Personal data may be transferred to Cora Systems US Inc. in the United States and jurisdictions where Cora's Subprocessors and affiliates operate.

b) To the extent such global processing involves the transfer of Personal Data which is subject to regulation and restriction on cross-border transfers under Applicable Data Protection Law, Cora shall put appropriate safeguards in place in accordance with applicable law including Standard Contractual Clauses where necessary.

11 Breach notices

Cora will notify Customer without undue delay after becoming aware of a data Breach that may put the confidentiality or security of the Personal Data in jeopardy. In such an event, Cora will collaborate with Customer and fulfil any reasonable requests by Customer for updates so long as such requests do not interfere with Cora's investigation and mitigation of the effects of the breach.

12 Compliance Requirements

If Cora is required by law to provide access to Personal Data such as in compliance with a subpoena, court order, or other government requests, Cora will inform Customer of such a request to the extent such notice is reasonably practicable and permitted by law.

13 Data Protection Contact

Data Protection queries and communications may be submitted to the Cora privacy team at: info@corasystems.com

14 Additional European Data provisions

This Clause 14 shall apply only with respect to Cora's Processing of European Data in providing the Services.

a) Customer may provide Instructions to Cora with respect to data transfers, assistance with Data Subject requests to delete, erase, access, restrict, rectify, transmit, block access to, or object to the Personal Data Processing.

b) Cora will inform Customer in the event it believes Customer has provided unlawful Instructions.

c) Subject to the terms and conditions in this CDPA, the SSA, and the Sales Order, Customer grants Cora general permission to engage Subprocessors in the performance of the Services. These Subprocessors are identified in the customer portal.

d) Cora shall provide Customer notice prior to changing Subprocessors through the following procedure. Cora shall post an amended list of Subprocessors to the customer portal listing the additional replacement Subprocessor and send Customer email notice of the same (the "Subprocessor Change"). Such Subprocessor Change shall be deemed accepted by Customer 30 days after such notice unless Customer first gives Cora written notice of an objection to such change. Such objection shall provide justifiable grounds for the objection relating to the ability of the new Subprocessor to adequately protect Personal Data in accordance with this CDPA or Applicable Data Protection Law. In this event, the parties shall negotiate in good faith to find a mutually acceptable resolution. In the event Cora determines in its sole discretion that a resolution cannot be reached, (i) Customer may terminate the relevant services upon serving 30 days prior notice, and (ii) Cora may at its option terminate the Services immediately. In the event of early termination under this Clause, neither party shall have any liability to the other except that Customer shall not be relieved from payment obligations under the SSA for fees accrued up to the date of termination. If the termination under this Clause relates to part and not to the whole of the Services under a Sales Order, then Customer shall enter into a replacement Sales Order to reflect such partial termination.

e) Cora will provide reasonable assistance to Customer with any data protection impact assessments (DPIA's) and prior consultations with competent data privacy authorities to the extent required by European Data Protection Laws.

f) Customer may include the contact details of Customer's Data Protection Officer in their Sales Order.

g) Further details of Processing of European Data can be found in Appendix 1.

15 Additional Provisions for California Personal Data

This Clause 15 (Additional Provisions for California Personal Data) shall apply only with respect to California Personal Data.

a) When processing California Personal Data in accordance with your Instructions, the parties agree that Customer is a Business and Cora is a Service Provider for the purposes of the CCPA ("Business" and "Service Provider" are as defined in the CCPA).

b) The parties agree that Cora will Process the California Personal Data as a Service Provider for the purpose of performing the Services under the SSA or as otherwise permitted by the CCPA.

16 General Terms

a) The term of this CDPA shall be the Subscription Term of the SSA.

b) Notwithstanding anything else to the contrary in the SSA, Cora reserves the right to update and amend this CDPA and the SSA Clause 26 (Amendment) shall apply.

c) If any provision of this Agreement is deemed unenforceable for any reason, the unenforceable provision shall be amended to the extent permitted by law to achieve as nearly as possible the same intent and economic effect as the original provision and the remainder of the Agreement shall continue in full force and effect.

d) The liability of each party, taken in the aggregate, arising out of or related to this CDPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in Clause 20 (Liability) in the SSA and any reference in such section to the liability of a party means the aggregate liability of that party under the Agreement (including this CDPA). In no event shall this clause be interpreted to limit either party's liability with respect to any individual's data protection rights under this CDPA or otherwise.

e) This CDPA shall be governed by and construed in accordance with the laws of the Republic of Ireland unless required otherwise by applicable data protection laws.

f) Prior Versions: For earlier versions of this CDPA, please contact info@corasystems.com.

Appendix 1

Details of Processing

Subject matter	Personal Data is processed for the purpose of providing Project Portfolio Management product and services for the Controller to use for planning, maintaining and managing projects.
Duration of Processing Activities	Processing shall occur during the Subscription Term of the SSA and for 30 days thereafter.
Nature and Purpose of the Processing Activities	Cora may Process Personal Information as necessary to perform the Services, including storage, backup and disaster recovery; providing technical support and processing change orders; updating the system and applying new system versions, patches, and upgrades; monitoring and testing system use and performance; performing incident management, maintenance, configuration, IT infrastructure maintenance and troubleshooting, migration, implementation, and performance testing of the system.
Types of Personal Data	Types of Personal Data may include First name, surname, email address, username.
Categories of Data Subject	Categories may include staff, employees, personnel, contractors, suppliers, end users.
Additional Information	Where requested, additional or more specific Processing descriptions may be set out in the SSA.