Data Processing Agreement for Aconex Cloud Services

Version December 4, 2018

1. Scope, duration and description of Processing

This Data Processing Agreement for Aconex Cloud Services (the “Data Processing Agreement”) details the parties’ obligations regarding the Processing of Personal Information on your behalf [hereinafter “Client”] as part of the provision of Aconex Cloud Services as described in further detail in the Aconex Terms of Service Agreement (hereinafter “Agreement”).

The description of Processing, including a description of the Processing activities and categories of Personal Information and Data Subjects, is set out in Exhibit 1 to this Data Processing Agreement. The duration and any additional details on the categories of Personal Information and Data Subjects are specified in the Agreement. In the event of a conflict between the terms of the Agreement and that of this Data Processing Agreement, the terms of this Data Processing Agreement shall prevail. In the event of any conflict between this Data Processing Agreement, and EU Model Clauses (defined in Section 7 below), the relevant terms of the EU Model Clauses shall take precedence. Unless otherwise expressly stated in the Services Order or the Agreement, this version of the Data Processing Agreement is incorporated into and subject to the terms of the Agreement, and shall be effective and remain in force for the term of the Services Order.

For the purpose of this Data Processing Agreement the following terms will have the same meaning as assigned under the Regulation (EU) 2016/679 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 (“GDPR”) or other data privacy or data protection law or regulation that applies to the Processing of Personal Data under this Data Processing Agreement (such laws collectively with GDPR, “Applicable Data Protection Law”): “Data Subject”, “Process/Processing”, “Personal Information” or “Personal Data”, “Supervisory Authority”, “Controller”, “Processor” and “Binding Corporate Rules” (or any of the equivalent terms).

2. Purpose of Processing and Responsibilities

Unless otherwise required by Applicable Data Protection Law, Aconex shall Process Personal Information as a Processor on behalf of Client for the purpose of rendering the Aconex Cloud Services in accordance with this Data Processing Agreement and its Processor obligations under Applicable Data Protection Law.

Client is responsible for (1) complying with its obligations as a Controller under this Data Processing Agreement and Applicable Data Protection Law, including the lawfulness of disclosing Personal Information to Aconex and (2) providing any required notices and notifications to any applicable co-Controllers that have been granted access to the Aconex Services and ensuring any required authorizations have been obtained in relation to any co-Controller rights under this Data Processing Agreement that are exercised through Client.

3. Client Instructions

Client’s instructions regarding the Processing of Personal Data are reflected in the Agreement and this Data Processing Agreement. Client has the right to reasonably provide additional instructions to Aconex regarding the Processing of Personal Data. If the exercise of the right to issue reasonable instructions results in disproportionate efforts on part of Aconex which exceed the Services set forth in the Agreement or Aconex' duties under Applicable Data Protection Law, Aconex may comply with the instruction for a separate fee in relation to the efforts arising thereof.

Where Aconex believes that an instruction would be in breach of Applicable Data Protection Law, Aconex shall notify Client of such belief without undue delay. However, Client acknowledges that Aconex is not responsible for providing legal advice to Client.

4. **Security and Confidentiality of Processing**

Aconex shall implement appropriate technical and organisational security measures designed to ensure the confidentiality, integrity, availability of Personal Information, and to protect Personal Information against unauthorized Processing activities. Aconex shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures which are designed to ensure the security of the processing by way of audits and assessments conducted by independent third-party auditors. Additional details regarding these security controls may be specified in the Agreement.

Aconex undertakes that all its employees involved in Processing of Personal Information and other such persons as may be involved in such Processing shall be prohibited from Processing Personal Information outside the scope of the Agreement and are subject to written confidentiality arrangements. Furthermore, Aconex undertakes that any person entitled to Process Personal Information has undertaken a commitment to confidentiality or is subject to an appropriate confidentiality obligation.

5. **Personal Information Breach Notification**

Aconex shall promptly notify Client if Aconex becomes aware of and determines that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed under the Agreement has occurred that compromises the security, confidentiality or integrity of such Personal Information Processed by within Aconex's scope of responsibility ("Personal Information Breach"). Aconex will provide Client with (i) a description of the nature and reasonably anticipated consequences of the Personal Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Information and Data Subjects including an approximate number of Personal Information records and Data Subjects that were the subject of the Personal Information Breach; and (iv) other information concerning the Personal Information Breach reasonably known or available to Aconex that Client may be required to disclose to a Supervisory Authority or affected Data Subject(s).

Aconex shall implement reasonable measures designed to mitigate potential adverse consequences of the Personal Information Breach. Within the timeframes required for Client to meet its Personal Data Breach notification obligations under Applicable Data Protection Law, Client agrees to coordinate with Aconex in good faith on the content of Client's intended public statements or required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authorities regarding the Personal Information Breach.

6. **Data Subject Requests**

Aconex shall reasonably support Client to enable Client to respond to Data Subject requests submitted in accordance with Applicable Data Protection Law.

Where a Data Subject makes a request under Applicable Data Protection Law directly to Aconex, Aconex shall refer such Data Subject to Client promptly without responding to such request, to the extent the Data Subject has identified Client as the Controller. Otherwise, Aconex shall advise the Data Subject to identify and contact the relevant controller.

7. **Audit rights**

Client may request in writing that Aconex provide to Client any applicable and available audit reports to help enable Client to confirm Aconex's compliance with its obligations under this Data Processing Agreement.

To the extent required by Applicable Data Protection Law, including where mandated by a Supervisory Authority, Client is entitled to conduct up to once per year an audit to confirm compliance with the relevant controls under this Data Processing Agreement . Such audits and inspections will be conducted during regular business hours, and without interfering with Aconex's operations, upon at least 28 days prior notice and pursuant to an agreed-upon scope. If Client would like a third party to conduct the audit, the third party must be mutually agreed to by the parties (except if such third party is a competent Supervisory Authority), and must execute a written confidentiality agreement acceptable to Aconex.

The audit report or findings shall be confidential information under the Agreement and Client will provide Aconex with a copy thereof. Client may use the audit reports and findings only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, or similar audit report issued by a qualified third party auditor within the prior twelve months and Aconex provides such report to Client confirming there are no known material changes in the controls audited, Client agrees to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

Each party will bear its own costs in relation to the audit, unless Aconex promptly informs Client upon reviewing the audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees for Aconex Cloud Services payable under the Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

8. **Data Transfers**

Aconex may Process Personal Information on a global basis as necessary to perform the Services, including for IT security purposes, maintenance and performance of the Services and related infrastructure, and technical support.

To the extent such global access involves a transfer of Personal Information originating from the European Economic Area ("EEA") or Switzerland to Aconex or Oracle affiliates and/or third party subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national EEA data protection authority, such transfers are subject to (i) the terms of the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision ("EU Model Clauses") incorporated into this Data Processing Agreement by reference; or (ii) other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Applicable Data Protection Law, such as approved Binding Corporate Rules for Processors. For the purposes of the EU Model Clauses, Client and Aconex agree that (i) Client will act as the data exporter on Client's own behalf and on behalf of any of Client's entities, (ii) Aconex will act on its own behalf and/or on behalf of the relevant Aconex affiliates as the data importers, (iii) any third party subprocessors will act as 'subcontractors' pursuant to Clause 11 of the EU Model Clauses.

Transfers of Personal Information originating from other locations globally to Aconex affiliates or third party subprocessors are subject to (i) for Aconex affiliates, the terms of the EU Model Clauses for Controllers; and (ii) for third party subprocessors, the terms of the relevant Aconex third party subprocessor agreement incorporating security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement.

9. **Subprocessors**

Aconex may engage Aconex and Oracle affiliates and third party subprocessors to help deliver the Aconex Cloud Services.

Client hereby consents to Aconex's use of such subprocessors. Aconex will promptly provide the current list of subprocessors upon Client's first request, which may be submitted via privacy@aconex.com.

Within fourteen (14) calendar days of Aconex providing such list to Client, Client may object to the intended involvement of a third party subprocessor in the performance of the Services, providing objective justifiable grounds related to the ability of such third party subprocessor to adequately protect Personal Information in accordance with this Data Processing Agreement or Applicable Data Protection Law in writing via privacy@aconex.com, or other applicable primary support tool provided for the Services. In the event Client's objection is justified, Client and Aconex will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the third party subprocessors' compliance with this Data Processing Agreement or applicable data protection law, or delivering the Services without the involvement of such third party subprocessor. To the extent Client and Aconex do not reach a mutually acceptable resolution within a reasonable timeframe, Client shall have the right to terminate the relevant Services (i) upon serving prior notice in accordance with the terms of the Agreement; (ii) without liability to Client and Aconex and (iii) without relieving Client from Client's payment obligations under the Agreement up to the date of termination. If the termination in accordance with this Section 9 only pertains to a portion of Services under an order, Client will enter into an amendment or replacement order to reflect such partial termination.

Where Aconex commissions subprocessors, Aconex shall be responsible for ensuring that Aconex's obligations on data protection resulting from the Agreement and this Data Processing Agreement are valid and binding upon subprocessor and Aconex shall remain responsible to Client for the performance of any subprocessor engaged by Aconex.

10. **Return and Deletion of Personal Information**

For a period of 60 days after the termination or expiration of the Aconex Cloud Services under Client's order, Aconex will make available Client's Personal Information via secured protocols, or keep Client's access to the production Aconex Cloud Services environment accessible, for the purpose of Personal Information retrieval by Client ("Retrieval Period"). During the Retrieval Period, Client should not use the environment for production activities.

At the latest within 120 days upon expiration the Retrieval Period following such Aconex Cloud Services, Aconex will disable Client's access to the production Aconex Cloud Services environment and will delete Client's Personal Information residing in the production environment, except as may otherwise be required by law.

11. **Legally Required Disclosure Requests**

If Aconex receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the Processing of Personal Information ("Disclosure Request"), it will promptly pass on such Disclosure Request to Client without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

At Client's request, Aconex will provide Client with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for Client to respond to the Disclosure Request in a timely manner.

12. **Data Protection Officer**

Aconex has appointed a Global Data Protection Officer. Further details on how to contact Aconex's Global Data Protection Officer are available here.

If Client has appointed a Data Protection Officer, Client may request Aconex to include the contact details of Client's Data Protection Officer in the relevant Services Order.

Exhibit 1: Description of Processing

Nature and purpose of data collection, processing or use:
Aconex provides software and services for construction project and property management which involves processing personal information provided by Client in accordance with the terms of the Agreement.

Categories of personal information that may be Processed:
First and last name; employer; business role; professional title; contact information (e.g., email, phone, physical address).

Categories of data subjects whose Personal Information may be Processed:
Clients and prospects of the data exporter; employees or contractors of the data exporters' prospects and Clients, and; employees and contractors of the Client.