Data Processing Agreement for Oracle Cloud Services

Version July 27, 2018

1. Scope, Order of Precedence and Term

1.1 This data processing agreement (the "Data Processing Agreement") applies to Oracle's Processing of Personal Data on Your behalf as part of Oracle's provision of Oracle Cloud Services ("Cloud Services"). The Cloud Services are described in (i) the applicable order for Cloud Services, (ii) the applicable Agreement or other applicable master agreement by and between You and Oracle in which this Data Processing Agreement is referenced, and (iii) the Service Specifications (i, ii and iii collectively the "Cloud Services Agreement").

1.2 Unless otherwise expressly stated in the order for Cloud Services, this version of the Data Processing Agreement is incorporated into and subject to the terms of the Cloud Services Agreement, and shall be effective and remain in force for the Service Period of the Cloud Services.

1.3 Except as expressly stated otherwise in this Data Processing Agreement or the order for Cloud Services, in the event of any conflict between the terms of the Cloud Services Agreement, including any policies or schedules referenced therein, and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall take precedence. In the event of any conflict between this Data Processing Agreement, and EU Model Clauses or the Argentinian Model Clauses, the relevant terms of the EU Model Clauses or the Argentinian Model Clauses shall take precedence.

2. Definitions

2.1 "Applicable Data Protection Law" means (i) 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"); (ii) all relevant European Union member state laws or regulations supplementing the GDPR; and (iii) any other data privacy or data protection law or regulation that applies to the Processing of Personal Data under this Data Processing Agreement.

2.2 "You" means the customer entity that has executed the order for Cloud Services.

2.3 "Data Subject", "Data Protection Officer", "Process/Processing", "Personal Data", "Supervisory Authority", "Controller", "Processor" and "Binding Corporate Rules" (or any of the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

2.4 **"**EU Model Clauses" means 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.

2.5 "Argentinean Model Clauses" means the Model Agreement of International Transfer of Personal Data for the case of Personal Data Assignment (*Contrato modelo de transferencia internacional de datos*

personales con motivo de la cesión de datos personales), approved by the National Directorate for Personal Data Protection on 2 November 2016.

2.6 “Oracle” means the Oracle Affiliate that has executed the order for Cloud Services.

2.7 “Oracle Affiliate(s)” means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Data as set forth in Sections 3.3 and 8.

2.8 “Third Party Subprocessor” means a third party subcontractor, other than an Oracle Affiliate, engaged by Oracle and which may Process Personal Data as set forth in Sections 3.3 and 8.

2.9 Other capitalized terms have the definitions provided for them in the Cloud Services Agreement or as otherwise specified below.

3. Controller and Processor of Personal Data and Purpose of Processing

3.1 You are and will at all times remain the Controller of the Personal Data Processed by Oracle under the Cloud Services Agreement. You are responsible for compliance with Your obligations as a Controller under Applicable Data Protection Law, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law).

3.2 Oracle is and will at all times remain a Processor with regard to the Personal Data provided by You to Oracle under the Cloud Services Agreement. Oracle is responsible for compliance with its obligations under this Data Processing Agreement and for compliance with its obligations as a Processor under Applicable Data Protection Law.

3.3 Oracle and any persons acting under the authority of Oracle, including any Oracle Affiliates and Third Party Subprocessors as set forth in Section 8, will Process Personal Data solely for the purpose of (i) providing the Cloud Services in accordance with the Cloud Services Agreement and this Data Processing Agreement, (ii) complying with Your documented written instructions in accordance with Section 5, and/or (iii) complying with Oracle’s regulatory obligations in accordance with Section 13.

4. Categories of Personal Data and Data Subjects

4.1 In order to perform the Cloud Services and depending on the Cloud Services You have ordered, Oracle may Process some or all of the following categories of Personal Data: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

4.2 Categories of Data Subjects whose Personal Data may be Processed in order to perform the Cloud Services may include, among others, Your representatives and end users, such as Your employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

4.3 Additional or more specific categories of Personal Data and/or Data Subjects may be described in the Cloud Services Agreement. Unless otherwise specified in the Cloud Services Agreement, Your Content may not include any sensitive or special personal data that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Service Specifications.

5. Your Instructions

5.1 Oracle will Process Personal Data on Your written instructions as specified in the Cloud Services Agreement and this Data Processing Agreement, including instructions regarding data transfers as set forth in Section 7.

5.2 You may provide additional instructions in writing to Oracle with regard to Processing of Personal Data in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Cloud Services, including assistance with notifying Personal Data Breaches as set forth in Section 11, Data Subject requests as set forth in Section 6, implementing appropriate technical and organizational measures as set forth in Section 9, data protection impact assessments and prior consultations as set forth in Section 10.8.

5.3 To the extent required by Applicable Data Protection Law, Oracle will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. You acknowledge and agree that Oracle is not responsible for performing legal research and/or for providing legal advice to You.

5.4 Oracle will comply with Your instructions at no additional cost to You. To the extent, Oracle expects to incur additional charges or fees not covered by the fees for Cloud Services payable under the Cloud Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

6. Rights of Data Subjects

6.1 Oracle will grant You electronic access to Your Cloud Services environment that holds Personal Data to enable You to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law, including requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Data or sets of Personal Data.

6.2 To the extent such electronic access is not available to You, You can submit a "service request" via My Oracle Support (or other applicable primary support tool provided for the Cloud Services), and provide detailed written instructions to Oracle (including the Personal Data necessary to identify the Data Subject) on how to assist with such Data Subject requests in relation to Personal Data held in Your Cloud Services environment. Subject to Section 5.4 and taking into account the nature of the Processing, Oracle will promptly follow such instructions within the timeframes reasonably necessary for You to respond to such Data Subject requests under Applicable Data Protection Law.

6.3 If Oracle directly receives any requests from Data Subjects that have identified You as the Data Controller, it will promptly pass on such requests to You without responding to the Data Subject. If the

Data Subject does not identify You as the Data Controller, Oracle will instruct the Data Subject to contact the relevant Data Controller.

7. Personal Data Transfers

7.1 Personal Data held in Your Cloud Services environment will be hosted in the data center region specified in the Cloud Services Agreement or otherwise selected by You. Oracle will not migrate Your Cloud Services environment to a different data center region without Your prior written authorization.

7.2 Without prejudice to Section 7.1 and in accordance with Your instructions under Section 5.1, Oracle may access and Process Personal Data on a global basis as necessary to perform the Cloud Services, including for IT security purposes, maintenance and performance of the Cloud Services and related infrastructure, Cloud Services technical support and Cloud Service change management.

7.3 To the extent such global Processing involves a transfer of Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Law in the European Economic Area ("EEA") or Switzerland to Oracle Affiliates 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 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, You and Oracle agree that (i) You will act as the data exporter on Your own behalf and on behalf of any of Your entities, (ii) Oracle will act on its own behalf and/or on behalf of the relevant Oracle Affiliates as the data importers, and (iii) any Third Party Subprocessors will act as 'subprocessors' pursuant to Clause 11 of the EU Model Clauses.

7.4 To the extent such global Processing involves a transfer of Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Law in Argentina to Oracle Affiliates or Third Party Subprocessors located in countries outside Argentina that have not received a binding adequacy decision by the National Directorate for Personal Data Protection, such transfers are subject to (i) the terms of the Argentinean 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.

7.5 Transfers of Personal Data subject to cross-border transfer restrictions under Applicable Data Protection Law in other locations globally to Oracle Affiliates or Third Party Subprocessors are subject to (i) for Oracle Affiliates, the terms of the Oracle Intra-Company Data Processing and Transfer Agreement entered into between Oracle Corporation and the Oracle Affiliates, which requires all transfers of Personal Data to be made in compliance with all applicable Oracle security and data privacy policies and standards and an applicable transfer mechanism as set forth in Section 7.3; and (ii) for Third Party Subprocessors, the terms of the relevant Oracle Third Party Subprocessor agreement incorporating security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

7.6 The terms of this Data Processing Agreement shall be read in conjunction with the EU Model Clauses, the Argentinean Model Clauses and other applicable transfer mechanisms pursuant to this Section 7.

8. Oracle Affiliates and Third Party Subprocessors

8.1 Subject to the terms and restrictions specified in Sections 3.3, 7 and 8, You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors to assist in the performance of the Cloud Services.

8.2 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Data. These lists are available to You via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool provided for the Cloud Services, such as the NetSuite Support Portal). If You would like to receive notice of any intended changes to these lists, You can sign up per the instructions on My Oracle Support, Document ID 2288528.1 or Oracle will provide you notice of intended changes where a sign up mechanism is not available.

8.3 Within fourteen (14) calendar days of Oracle providing such notice to You, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Cloud Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Data in accordance with this Data Processing Agreement or Applicable Data Protection Law in writing by submitting a "service request" via My Oracle Support, or other applicable primary support tool provided for the Cloud Services. In the event Your objection is justified, You and Oracle 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' or Oracle Affiliate's compliance with this Data Processing Agreement or Applicable Data Protection Law, or delivering the Cloud Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Cloud Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You and Oracle and (iii) without relieving You from Your payment obligations under the Cloud Services Agreement up to the date of termination. If the termination in accordance with this Section 8.3 only pertains to a portion of Cloud Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

8.4 The Oracle Affiliates and Third Party Subprocessors are required by written agreement to abide by the same level of data protection and security as Oracle under this Data Processing Agreement as applicable to their Processing of Personal Data. You may request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with such obligations. You will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Data.

8.5 Oracle remains responsible at all times for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

9. Technical and Organizational Measures, and Confidentiality of Processing

9.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data. These measures take into account the nature, scope and purposes of Processing as specified in this Data Processing Agreement, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the

Cloud Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

9.2 In particular, Oracle has implemented the physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures specified in the relevant Cloud Services Hosting and Delivery Policies and other Service Specifications. You are advised to carefully review the applicable Service Specifications to understand which specific security measures and practices apply to the particular Cloud Services ordered by You, and to ensure that these measures and practices are appropriate for the Processing of Personal Data pursuant to this Data Processing Agreement.

9.3 All Oracle and Oracle Affiliate staff, as well as any Third Party Subprocessors that Process Personal Data are subject to appropriate written confidentiality arrangements.

10. Audit Rights and Cooperation with You and Your Supervisory Authorities

10.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, including where mandated by Your Supervisory Authority, You or Your Supervisory Authority may perform more frequent audits, including inspections of the Cloud Service data center facility that Processes Personal Data. Oracle will contribute to such audits by providing You or Your Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including by making available a record of Processing activities and other information as further described in Section 10.8.

10.2 If a third party is to conduct the audit, the third party must be mutually agreed to by You and Oracle (except if such Third Party is a competent Supervisory Authority). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

10.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions (for example, any request for information that could compromise Oracle security, privacy, employment or other relevant policies). Oracle will work cooperatively with You to agree on a final audit plan.

10.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

10.5 You will provide Oracle any reports generated in connection with any audit under this Section 10, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement. The audit reports are Confidential Information under the terms of the Cloud Services Agreement.

10.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your 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 Cloud Services payable under the Cloud Services 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.

10.7 Without prejudice to the rights granted in Section 10.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree 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.

10.8 Oracle provides you with information and assistance reasonable necessary for You to conduct Your data protection impact assessments or consult with Your Supervisory Authorities, by granting You electronic access to a record of Processing activities and any available privacy & security functionality guides for the Cloud Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Cloud Services, such as the NetSuite Support Portal, or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to You.

11. Incident Management and Personal Data Breach Notification

11.1 Oracle promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or Processing of Personal Data ("Incident"). All Oracle and Oracle Affiliates staff that have access to or Process Personal Data are instructed on responding to Incidents, including prompt internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence. Oracle's agreements with Third Party Subprocessors contain similar Incident reporting obligations.

11.2 In order to address an Incident, Oracle defines escalation paths and response teams involving internal functions such as Information Security and Legal. The goal of Oracle's Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Oracle may also involve and work with You and outside law enforcement to respond to the Incident.

11.3 To the extent Oracle becomes aware and determines that an Incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Oracle systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such Personal Data ("Personal Data Breach"), Oracle will inform You of such Personal Data Breach without undue delay but at the latest within 24 hours.

11.4 Oracle will take reasonable measures designed to identify the root cause(s) of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Oracle and to the extent permitted by law, Oracle will provide You with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Data and Data Subjects including an approximate number of Personal Data records and Data Subjects that were the subject of the Personal Data Breach; and (iv) other information concerning the Personal Data Breach

reasonably known or available to Oracle that You may be required to disclose to a Supervisory Authority or affected Data Subject(s).

11.5 Within the timeframes required for You to meet Your Personal Data Breach notification obligations under Applicable Data Protection Law, You agree to coordinate with Oracle in good faith on the content of Your intended public statements or required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authorities regarding the Personal Data Breach.

12. Return and Deletion of Personal Data upon Termination of Cloud Services

12.1 Following termination of the Cloud Services, Oracle will return or otherwise make available for retrieval Your Personal Data then available in Your Cloud Services environment, unless otherwise expressly stated in the Service Specifications. For Cloud Services for which no data retrieval functionality is provided by Oracle as part of the Cloud Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Data while the production Cloud Services environment is still active prior to termination.

12.2 Following any applicable retrieval period, Oracle will promptly delete all copies of Personal Data from the Cloud Services environment, except as may be required by law. Oracle's data deletion practices, as well as any applicable retention or archival practices, are described in more detail in the relevant Cloud Services Hosting and Delivery Policies and other Service Specifications applicable to the Cloud Services.

13. Legally Required Disclosure Requests

13.1 If Oracle 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 Data ("Disclosure Request"), it will promptly pass on such Disclosure Request to You 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).

13.2 At Your request, Oracle will provide You with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for You to respond to the Disclosure Request in a timely manner.

14. Data Protection Officer

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

14.2 If You have appointed a Data Protection Officer, You may request Oracle to include the contact details of Your Data Protection Officer in the relevant order for Cloud Services.