# Data Processing Agreement for Oracle Cloud Services

## Version March 1, 2017

### 1. Scope and order of precedence

This data processing agreement (the “Data Processing Agreement”) applies to Oracle’s Processing of Personal Data provided to Oracle by Customer as part of Oracle’s provision of Cloud Services (“Cloud Services”). The Cloud Services are specified in (i) the applicable Oracle Cloud Services Agreement or other applicable master agreement and (ii) the Oracle Cloud Order and all documents, addenda, schedules and exhibits incorporated therein (collectively the “Agreement”) by and between Customer and the Oracle subsidiary listed in the Oracle Cloud Order.

This Data Processing Agreement is incorporated into and subject to the terms of the Agreement. Except as expressly stated otherwise, in the event of any conflict between the terms of the 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.

This Data Processing Agreement shall be effective for the Service Period of any Oracle Cloud order placed under the Agreement.

### 2. Definitions

“Controller” and “Processor” have the meaning set forth in the Directive.

“Customer” means the Customer that has executed the Oracle Cloud Order.

“Data Subject” means an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

“Directive” means Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.

**“**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.

“Oracle” or “Processor” means the Oracle subsidiary listed in the Oracle Cloud Order.

“Oracle Affiliates” mean the subsidiaries of Oracle Corporation that may assist in the performance of the Cloud Services.

“Personal Data” means any information relating to a Data Subject that Customer or its end users provide to Oracle as part of the Cloud Services.

“Process” or “Processing” means any operation or set of operations which is performed by Oracle as part of the Cloud Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“Third Party Subprocessor” means a third party subcontractor, other than an Oracle Affiliate, engaged by Oracle which, as part of the subcontractor's role of delivering the Cloud Services, will Process Personal Data of the Customer.

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

### 3. Categories of Personal Data

In order to execute the Agreement, and in particular to perform the Cloud Services, Customer authorizes and requests that Oracle Process the following Personal Data:

Categories of Personal Data: Personal Data may include, among other information, 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, social security details 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.

Categories of Data Subjects: Data subjects may include Customer's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, customers and users of the Customer. Data subjects also may include individuals attempting to communicate or transfer Personal Data to users of the Cloud Services.

### 4. Customer's Instructions

Customer may provide instructions in writing to Oracle in addition to those specified in the Agreement with regard to Processing of Personal Data. Oracle will comply with all such instructions without additional charge to the extent necessary for Oracle to comply with its obligations as a Processor in the performance of the Cloud Services. The parties will negotiate in good faith with respect to any other change in the Cloud Services and/or fees resulting from any additional instructions.

### 5. Controller and Processor of Personal Data and purpose of the Personal Data Processing

Customer will at all times remain the Controller for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Customer is responsible for compliance with its obligations as a Controller under data protection laws, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents and authorizations), and for its decisions and actions concerning the Processing and use of the Personal Data.

Oracle is a Processor for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Oracle will Process Personal Data solely for the provision of the Cloud Services, and will not otherwise (i) Process or use Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in accordance with Section 4, or (ii) disclose such Personal Data to third parties other than Oracle Affiliates or Third Party Subprocessors for the aforementioned purposes or as required by law.

Oracle will comply with all applicable data protections laws to the extent that such laws by their terms impose obligations directly upon Oracle as a Processor in connection with the services specified in the applicable Cloud Order.

### 6. Rights of Data Subjects

Oracle will grant Customer electronic access to Customer's Cloud Services environment that holds Personal Data to permit Customer to respond to Data Subject requests to access, delete, release, correct or block access to specific Personal Data.

To the extent such electronic access is not available to Customer, Oracle will follow Customer's detailed written instructions to access, delete, release, correct or block access to Personal Data held in Customer's Cloud Services environment. Customer agrees to pay Oracle's reasonable fees that may be associated with Oracle's performance of any such access, deletion, release, correction or blocking of access to Personal Data on behalf of Customer.

Oracle will pass on to the Customer any requests of an individual Data Subject to access, delete, release, correct or block Personal Data Processed under the Agreement. Oracle will not be responsible for responding directly to the request, unless otherwise required by law.

## 7. Cross Border and Onward Data Transfers

Oracle treats all Personal Data in a manner consistent with the requirements of the Agreement and this Data Processing Agreement in all locations globally. Oracle's information, privacy and security policies, standards and governance practices are managed on a global basis.

Transfers of Personal Data originating from the 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 data protection authority, are subject to (i) the terms of the Model Clauses; or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the Directive. The terms of this Data Processing Agreement shall be read in conjunction with the Model Clauses or other appropriate transfer mechanisms.

Transfers of Personal Data originating from 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 (ii) for Third Party Subprocessors, the terms of the relevant Oracle Third Party Subprocessor agreement incorporating security and other data privacy requirements consistent with those of this Data Processing Agreement.

## 8. Affiliates and Third Party Subprocessors

Some or all of Oracle's obligations under the Agreement may be performed by Oracle Affiliates and Third Party Subprocessors. Oracle maintains a list of Oracle Affiliates and Third Party Subprocessors that may Process Personal Data. That list will be available to Customer via the Cloud portal or, to the extent Customer has no access to the Cloud portal, Oracle will provide a copy of that list to Customer upon request.

The Oracle Affiliates and Third Party Subprocessors are required to abide by substantially the same obligations as Oracle under this Data Processing Agreement as applicable to their Processing of Personal Data. Customer 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 ensure compliance with such obligations. Customer will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with Third Party Subprocessors that may Process Personal Data.

Oracle remains responsible at all times for compliance with the terms of this Data Processing Agreement by Oracle Affiliates and Third Party Subprocessors.

Customer consents to Oracle's use of Oracle Affiliates and Third Party Subprocessors in the performance of the Cloud Services in accordance with the terms of Sections 7 and 8 above.

## 9. Technical and Organizational Measures

Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data, including the measures specified in this Section to the extent applicable to Oracle's Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Cloud Services ordered by Customer, may be specified in the Agreement.

9.1 Physical Access Control. Oracle employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is Processed, such as the use of security personnel, secured buildings and data center premises.

9.2 System Access Control. The following may, among other controls, be applied depending upon the particular Cloud Services ordered: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Services hosted at Oracle: (i) log-ins to Cloud Services Environments by Oracle employees and Third Party Subprocessors are logged; (ii) logical access to the data centers is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.

9.3 Data Access Control. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. In addition to the access control rules set forth in Sections 9.1 – 9.3, Oracle implements an access policy under which Customer controls access to its Cloud Services environment and to Personal Data and other data by its authorized personnel.

9.4 Transmission Control. Except as otherwise specified for the Cloud Services (including within the Oracle Cloud Order or the applicable service specifications referenced in the Agreement), transmissions of data outside the Cloud Service environment are encrypted. Some Cloud Services, such as social media services, may be configurable by Customer to permit access to third party sites that require unencrypted communications. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. Customer is solely responsible for the results of its decision to use such unencrypted communications or transmissions.

9.5 Input Control. The Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer. As set forth in Section 9.4 above, note that some Cloud Services permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

9.6 Data Backup. For Cloud Services hosted at Oracle: back-ups are taken on a regular basis; back-ups are secured using a combination of technical and physical controls, depending on the particular Cloud Service.

9.7 Data Segregation. Personal Data from different Oracle customers' environments is logically segregated on Oracle's systems.

9.8 Confidentiality. All Oracle employees and Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements.

## 10. Audit Rights

Customer may audit Oracle's compliance with the terms of this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Cloud Service data center facility that Processes Personal Data to the extent required by laws applicable to Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and Oracle and must execute a written confidentiality agreement acceptable to Oracle before conducting the audit.

To request an audit, Customer must submit a detailed audit plan to Oracle at least two weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the audit plan and provide Customer 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 Customer to agree on a final audit plan. If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve months and Oracle confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

The audit must be conducted during regular business hours at the applicable facility, subject to Oracle policies, and may not unreasonably interfere with Oracle business activities.

Customer will provide Oracle any audit reports generated in connection with any audit under this Section 10, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits are at the Customer's expense. Any request for Oracle to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Cloud Services. Oracle will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

## 11. Incident Management and Breach Notification

Oracle evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or handling of Personal Data ("Incident"). Oracle operations staff is instructed on responding to Incidents where processing of Personal Data may have been unauthorized, including prompt and reasonable internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence.

Depending on the nature of the Incident, Oracle defines escalation paths and response teams to address the Incident. Oracle will work with Customer, with internal Oracle lines of business, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the Incident. The goal of Oracle's Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment, and to establish root causes and remediation steps.

For purposes of this section, "Security Breach" means the misappropriation or unauthorized Processing of Personal Data located on Oracle systems or the Cloud Services environment, including by an Oracle employee, that compromises the security, confidentiality or integrity of such Personal Data. Oracle will inform Customer within 24 hours or sooner as required by applicable law if Oracle determines that Personal Data has been subject to a Security Breach or any other circumstance in which Customer is required to provide a notification under applicable law.

Oracle will promptly investigate the Security Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by law, Oracle will provide Customer with a description of the Security Breach, the type of

Personal Data that was the subject of the Security Breach, and other information Customer may reasonably request concerning the affected Data Subjects. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant data protection authorities.

### 12. Return and Deletion of Personal Data upon End of Cloud Services

Following termination of the Cloud Services, Oracle will return or otherwise make available for retrieval Customer's Personal Data then available in the Customer's Cloud Services environment. Following return of such Personal Data, or as otherwise specified in the Agreement, Oracle will promptly delete or otherwise render inaccessible all copies of Personal Data from the production Cloud Services environment, except as may be required by law. Oracle's data return and deletion practices are described in more detail in the Agreement.

### 13. Legally Required Disclosures

Except as otherwise required by law, Oracle will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority ("Demand") that it receives and which relates to the Processing of Personal Data. At Customer's request, Oracle will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Oracle has no responsibility to interact directly with the entity making the Demand.

### 14. Service Analyses

Oracle may (i) compile statistical and other information related to the performance, operation and use of the Cloud Services, and (ii) use data from the Cloud Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (collectively "Service Analyses"). Oracle may make Service Analyses publicly available. However, Service Analyses will not incorporate Customer's Content, Personal Data or Confidential Information in a form that could identify or serve to identify Customer or any Data Subject. Oracle retains all intellectual property rights in Service Analyses.