Data Processing Agreement for Oracle Cloud Services

Version July 31, 2015

1. Scope and order of precedence

This 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"), as further specified in (i) the applicable Oracle master agreement and (ii) the Oracle Cloud Ordering Document between Customer and Oracle, and all documents, addenda, schedules and exhibits incorporated therein (collectively the "Agreement") by and between the Customer entity and Oracle subsidiary listed in the order for Cloud Services.

This Data Processing Agreement is subject to the terms of the Agreement and is incorporated into the Agreement. Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement 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 Services Period of any Oracle Cloud order placed under the Agreement.

2. Definitions

"Customer" or "you" means the Customer that has executed the order for Cloud Services.

"Oracle" or "Processor" means the Oracle subsidiary listed in the order for Cloud Services.

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

"Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 210/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive (defined below).

"Personal Data" means any information relating to an identified or identifiable natural person that Customer or its end users provide to Oracle as part of the Cloud Services; an identified or identifiable natural person (a "data subject") is one 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.

"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.

"Subprocessor" means a third party subcontractor engaged by Oracle which, as part of the subcontractor's role of delivering the Cloud Services, will Process Personal Data of the Customer.

"The 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.

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

3. Categories of Personal Data and purpose of the Personal Data Processing

In order to execute the Agreement, and in particular to perform the Cloud Services on behalf of Customer, 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; and goods and services provided.

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

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, or (ii) disclose such Personal Data to third parties other than Oracle Affiliates or Subprocessors for the aforementioned purposes or as required by law.

4. Customer's Instructions

During the Services Period of any order for Cloud Services, Customer may provide instructions 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 laws applicable to Oracle as a data 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 such instructions.

5. Controller of Data

The control of Personal Data remains with Customer, and as between Customer and Oracle, Customer will at all times remain the data controller for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Customer is responsible for compliance with its obligations as data 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 for its decisions and actions concerning the Processing and use of the data.

6. Rights of Data Subject

Oracle will grant Customer electronic access to Customer's Cloud Services environment that holds Personal Data to permit Customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to delete, release, correct or block access to Personal Data held in Customer's Cloud Services environment. Customer agrees to pay Oracle's reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to Personal Data. Oracle will pass on to the Customer any requests of an individual data subject to delete, release, correct or block Personal Data Processed under the Agreement.

7. Cross Border and Onward Data Transfer

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 policies, standards and governance practices are managed on a global basis.

With respect to Personal Data stored by Oracle in data centers in the United States managed by its affiliate Oracle America Inc., at all times during the performance of the Cloud Services, Oracle America Inc. will Process Personal Data originating from the European Economic Area (EEA) and/or Switzerland according to the relevant Safe Harbor Principles. Oracle America Inc. subscribes to the "Safe Harbor Principles" issued by the U.S. Commerce Department on July 21, 2000 and as a result, currently appears on the Department's Safe Harbor list (available at http://www.export.gov/safeharbor) as a member of both the United States-EU (European Union) and the United States-Swiss Safe Harbor Programs. Oracle has received the TRUSTe safe harbor seal, which is audited and renewed annually, and is part of the TRUSTe Safe Harbor Program. In the event of a lapse of Oracle's Safe Harbor status, Oracle will promptly remedy such a lapse or work with Customer to find an alternative means of meeting the adequacy requirements of the Directive.

With respect to Personal Data stored by Oracle in data centers in the EEA or in countries that have been subject to an adequacy (or equivalent) finding by the European Commission pursuant to Articles 25 and 26 of the Directive ("Adequacy Finding"), Oracle manages compliance by the Oracle Affiliates and by Subprocessors as follows. For Oracle Affiliates, Oracle Corporation and the Oracle Affiliates have entered into an intra-company agreement requiring compliance with the relevant Safe Harbor Principles and with all applicable Oracle security and data privacy policies and standards, including the requirement that transfers of Personal Data to Oracle Affiliates in or from countries that have not received an Adequacy Finding are made in compliance with the applicable requirements of Articles 25 and 26 of the Directive concerning international and onward data transfers. For Subprocessors, Oracle Corporation and the Oracle Affiliates have entered into contracts with Subprocessors that provide that the Subprocessor will undertake data protection and confidentiality obligations consistent with the Safe Harbor Principles and with the Oracle Supplier Security Standards. Where a Subprocessor Processes Personal Data in or from a country that has not received an Adequacy Finding, Oracle requires the Subprocessor to execute Model Clauses incorporating security requirements consistent with those of this Data Processing Agreement.

8. Affiliates and Subprocessors

Some or all of Oracle's obligations under the Agreement may be performed by Oracle Affiliates. Oracle and the Oracle Affiliates have entered into the intra-company agreement specified above, under which the Oracle Affiliates Processing Personal Data adopt safeguards consistent with those of Oracle. Oracle is responsible for its compliance and the Oracle Affiliates' compliance with this requirement.

Oracle also may engage Subprocessors to assist in the provision of the Cloud Services. Oracle maintains a list of Subprocessors that may Process the Personal Data of Oracle's Cloud Service customers and will provide a copy of that list to Customer upon request.

All Subprocessors are required to abide by substantially the same obligations as Oracle under this Data Processing Agreement as applicable to their performance of the Cloud Services. Customer may request that Oracle audit the 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 Subprocessor's operations) to ensure compliance with such obligations. Customer also will be entitled, upon written request, to receive copies of the relevant terms of Oracle's agreement with Subprocessors that may Process Personal Data, unless the agreement contains confidential information, in which case Oracle may provide a redacted version of the agreement.

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

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

9. Technical and Organizational Measures

When Processing Personal Data on behalf of Customer in connection with the Cloud Services, Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of such data, including the measures specified in this Section to the extent applicable to the 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 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 @Oracle: (i) log-ins to Cloud Services Environments by Oracle employees and 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 above, 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 ordering document or the applicable service specifications), transfers of data outside the Cloud Service environment are encrypted. Some Cloud Services, such as social media services, may be configurable to permit access to 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 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. 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 @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.

10. Audit Rights

Customer may audit Oracle's compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Cloud Service computer systems that Process 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 at least two weeks in advance of the proposed audit date to Oracle Corporation's Global Information Security organization ("GIS") describing 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 GIS any audit reports generated in connection with any audit under this section, 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 the Agreement and 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 unauthorized access to or handling of Personal Data ("Incident"). GIS is informed of such Incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those Incidents. GIS 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 the Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment, and to establish root causes and remediation steps.

Oracle operations staff is instructed on responding to Incidents where handling of Personal Data may have been unauthorized, including prompt and reasonable reporting to GIS and to Oracle Corporation's legal department, escalation procedures, and chain of custody practices to secure relevant evidence.

For purposes of this section, "Security Breach" means the misappropriation of Personal Data located on Oracle systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such information. Oracle will inform Customer within 72 hours if Oracle determines that Personal Data has been subject to a Security Breach (including by an Oracle employee) or any other circumstance in which Customer is required to provide a notification under applicable law, unless otherwise required by 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 data

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

12. Return and Deletion of Personal Data upon End of Cloud Services or at Customer's Request ("Data Portability")

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 the 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 or other governmental authority ("Demand") that it receives and which relates to the Personal Data Oracle is Processing on Customer's behalf. 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 (clauses i and ii are collectively referred to as "Service Analyses"). Oracle may make Service Analyses publicly available; however, Service Analyses will not incorporate Customer's Content or Confidential Information in a form that could identify or serve to identify Customer or any data subject, and Service Analyses do not constitute Personal Data. Oracle retains all intellectual property rights in Service Analyses.