Data Processing Agreement for Oracle Cloud Services

Version June 1, 2013

1. Scope and order of precedence

This is an agreement concerning the processing of Personal Data (as defined below) as part of the Oracle Cloud Services ("Services"), as further specified in (i) the applicable Oracle master agreement (e.g., the Oracle Cloud Services 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 your order for Cloud Services.

This agreement (the "Data Processing Agreement") is subject to the terms of the Agreement and is annexed as a schedule to the Agreement. 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 prevail. This Data Processing Agreement shall be effective for the Services Period of any order placed under the Oracle Cloud Services 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 your order for Cloud Services.

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

"Model Clauses" means the Standard Clauses for the Transfer of Personal Data to Processors in Third Countries under Directive 95/46 approved by Commission Decision of February 5, 2010, including Appendices 1 and 2 thereto.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable 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.

"The Directive" means Directive 95/46/EC 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 specificed 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 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 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 Services.

Oracle shall process Personal Data solely for the provision of the Services, and shall not otherwise (i) process and 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 its 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 Services; the parties will negotiate in good faith with respect to any other change in the Services and/or fees resulting from such instructions.

Oracle will inform Customer if, in Oracle's opinion, an instruction breaches data protection regulations. Customer understands that Oracle is not obligated to perform legal research and/or to provide legal advice to Customer.

5. Controller of Data

The control of Personal Data remains with Customer, and Customer will at all times remain the data Controller for the purposes of the 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 concerning the processing and use of the data.

6. Rights of Data Subject

Oracle will grant Customer electronic access to Customer's subscribed Cloud Services Environments that hold 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. Customer agrees to pay Oracle's reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to data. Oracle shall pass on to the Customer contacts identified in Section 15 below 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.

Oracle acknowledges that some data handled in providing the Services to the Customer may be Personal Data of, or related to, European Union (EU) data subjects. Where Oracle's processing of such Personal Data takes place in countries that have not received an "adequacy" finding pursuant to Articles 25 and 26 of the Directive, Oracle shall ensure that transfers of such Personal Data to Oracle Affiliates and contractors in such countries are made in compliance with the applicable requirements of Articles 25 and 26 of the Directive concerning international and onward data transfers.

With respect to 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 Services, Oracle America Inc. will process Personal Data originating from the European Economic Community

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 European Union – United States and Switzerland – United States 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 European Union, Oracle shall ensure compliance by the Oracle Affiliates and by subprocessors (defined below) with the requirements of this Section 7 as follows: (i) 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, and further permitting each Oracle Affiliate to enter into Model Clauses on behalf of Oracle Corporation and the remaining entities as necessary, and (ii) in the case of subprocessors assisting in the performance of the Services, by way of contracts with subprocessors having access to Personal Data which provide that the subprocessor will undertake data protection and confidentiality obligations consistent with the Safe Harbor principles and with the Oracle Supplier Security Standards; further, where a subprocessor accesses and processes Personal Data in a country that has not received an "adequacy" finding pursuant to Articles 25 and 26 of the Directive, Oracle will require 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 subscribed to the intra-company agreement specified above, under which an Oracle subsidiary handling Personal Data adopts safeguards consistent with those of the Oracle subsidiary contracting with a customer for Oracle Cloud Services. The Oracle Affiliate contracting with the customer is responsible for Oracle compliance and the Oracle Affiliates' compliance with this requirement.

Oracle also may engage third party subcontractors to assist in the provision of the Services. Oracle maintains a list of subcontractors that may have access to Personal Data of Oracle's Cloud Service customers ("subprocessors") 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 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 with access to Personal Data, unless the agreement contains confidential information, in which case Oracle may provide a redacted version of the agreement.

Oracle shall remain 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 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 Services, Oracle shall ensure that it implements and maintains compliance with appropriate technical and organizational security measures for the processing of such data. In particular, Oracle will implement the following measures:

9.1 To prevent unauthorized persons from gaining access to data processing systems in which Personal Data are processed or used (physical access control), Oracle shall take measures to prevent physical access, such as security personnel and secured buildings and factory premises.

9.2 To prevent data processing systems from being used without authorization (system access control), the following are applied: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. Log-ins to Cloud Services Environments by Oracle employees and subprocessors are logged. Llogical access to the data centers is restricted and protected by firewall/VLAN. In addition, currently the following security processes are applied: intrusion detection system, patch and vulnerabilities management, centralized logging and alerting, and firewalls. Logging is accomplished at system, platform and application levels.

9.3 To ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and that Personal Data cannot be read, copied, modified or removed without authorization in the course of processing or use and/or after storage (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 Services Environment and to Personal Data and other data by its authorized personnel.

9.4 To ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control), Oracle will comply with the following requirements: Except where otherwise specified in the Service Specifications, transfers of data outside the Service Environment are encrypted. Some Services, such as social media Services, may be configurable to permit access to sites that require non-encrypted communications. The content of communications (including sender and recipient addresses) sent through some email or messaging Services may not be encrypted once received through such Services. Customer is solely responsible for the results of its decision to use non-encrypted communications.

9.5 To ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed (input control), Oracle will comply with the following requirements: 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.

9.6 To ensure that the Personal Data are processed strictly in accordance with the instructions of the Customer, Oracle must comply with the instructions of the Customer concerning processing of Personal Data; such instructions are specified in the Agreement and in this Data Processing Agreement, and may additionally be provided by Customer in writing from time to time.

9.7 To ensure that Personal Data are protected against accidental destruction or loss, back-ups are taken on a regular basis; back-ups are encrypted and are secured.

9.8 To ensure that Personal Data which are collected for different purposes may be processed separately, data from different customers' environments is logically segregated on Oracle's systems.

Information concerning the specific security practices described in this Section 9 and employed as part of the Services is specified in the Service Specifications in effect as the Services are performed.

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. 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, or employment policies). Oracle will work cooperatively with Customer to agree on a final audit plan.

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. If the information required for such an audit is not contained in a SSAE 16/ISAE 3402 Type 2 or similar report, Oracle will make reasonable efforts to provide requested information to the auditor.

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 different or additional resources. 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. 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 electronic media that compromises the security, confidentiality or integrity of such information. Oracle shall promptly inform Customer 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 shall promptly investigate any 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.

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

Following termination of the Services, Oracle will promptly make customer's Personal Data as existing in the production Cloud Services Environment as of the date of termination available for export. Following return of the data, 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 practices are described in more detail in the Cloud Services Agreement and the Oracle Cloud Suspension and Termination Policies.

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 Services, and (ii) use data from the 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 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.

15. Communications

The person(s) or entity authorized by Customer to issue instructions under this Agreement are those specified as contacts under the order for Cloud Services. In the event that any of these contacts are changed or permanently unavailable, Customer must communicate this immediately to Oracle in writing, appointing a replacement.

Effective Date: June 1, 2013

Prior version(s) available [Data Processing Agreement v120112].