APPENDIX O TO DIR CONTRACT NO. DIR-TSO-4158

Legal Notices

Oracle Services Privacy Policy

Scope

This policy covers the privacy practices that Oracle Corporation and its subsidiaries and affiliates ("Oracle" or "we") employ when providing support, consulting, Cloud or other services (the "services") to its customers ("you" or "your"). Oracle established this privacy policy in order to clarify that the use of information to which it may be provided access in order to provide services is more limited than the use of information covered by Oracle's general privacy policy.

Customer Information and Services Data

Customer Information is information that we may collect from your use of the Oracle Web sites and your interactions with us offline. We deal with customer information according to the terms of our general privacy policy.

Services Data is data that resides on Oracle, customer or third-party systems to which Oracle is provided access to perform services (including Cloud environments as well as test, development and production environments that may be accessed to perform Oracle consulting and support services). Oracle treats services data according to the terms of this policy, and treats services data as confidential in accordance with the terms of your order for services.

To illustrate the difference between customer information and services data, when a customer contracts with Oracle for Cloud services, the customer provides information about itself, including its name, address, billing information, and some employee contact information. Oracle may also collect other information about the customer and some employees, for example through its web sites, as part of that interaction. All of that information is customer information, and is treated according to Oracle's general privacy policy.

In contrast, having contracted with Oracle for Cloud or other services, the customer provides Oracle access to its production, development or test environment, which may include personal information about its employees, customers, partners or suppliers (collectively "end users").

How Oracle Collects and Uses Services Data

Below are the conditions under which Oracle may access, collect and/or use services data.

To Provide Services and to Fix Issues. Services data may be accessed and used to perform services under your order for support, consulting, Cloud or other services and to confirm your compliance with the terms of your order. This may include testing and applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; and resolving bugs and other issues you have reported to Oracle. Any copies of services data created for these purposes are only maintained for time periods relevant to those purposes.

As a Result of Legal Requirements. Oracle may be required to retain or provide access to services data to comply with legally mandated reporting, disclosure or other legal process requirements.

Oracle may transfer and access services data globally as required for the purposes specified above. If Oracle hires subcontractors to assist in providing services, their access to services data will be consistent with the terms of your order for services and this services privacy policy. Oracle is responsible for its subcontractors' compliance with the terms of this policy and your order.

Oracle does not use services data except as stated above or in your order. Oracle may process services data, but does not control your collection or use practices for services data. If you provide any services data to Oracle, you are responsible for providing any notices and/or obtaining any consents necessary for Oracle to access, use, retain and transfer services data as specified in this policy and your order.

Access Controls

Oracle's access to services data is based on job role/responsibility. Services data residing in Oracle-hosted systems is controlled via an access control list (ACL) mechanism, as well as the use of an account management framework. You control access to services data by your end users; end users should direct any requests related to their personal information to you.

Security and Breach Notification

Oracle is committed to the security of your services data, and has in place physical, administrative and technical measures designed to prevent unauthorized access to that information. Oracle security policies cover the management of security for both its internal operations as well as the services. These policies, which are aligned with the ISO/IEC 27001:2013 standard, govern all areas of security applicable to services and apply to all Oracle employees. Oracle's Support, Consulting and Cloud lines of business have developed detailed statements of security practices that apply to many of their service offerings, which are available for review at your request.

Oracle's security policies and procedures are reviewed and overseen by Oracle Global Information Security (GIS). GIS is responsible for security oversight, compliance and enforcement, and for conducting information security assessments and leading the development of information security policy and strategy.

Oracle is also committed to reducing risks of human error, theft, fraud, and misuse of Oracle facilities. Oracle's efforts include making personnel aware of security policies and training employees to implement security policies. Oracle employees are required to maintain the confidentiality of services data. Employees' obligations include written confidentiality agreements, regular training on information protection, and compliance with company policies concerning protection of confidential information.

Oracle promptly evaluates and responds to incidents that create suspicions of unauthorized handling of services

data. Oracle GIS and Legal are informed of such incidents and, depending on the nature of the activity, define escalation paths and response teams to address the incidents. If Oracle determines that your services data has been misappropriated (including by an Oracle employee) or otherwise wrongly acquired by a third party, Oracle will promptly report such misappropriation or acquisition to you.

Cross Border Transfers

Oracle is a global corporation with operations in over 80 countries and has developed global data security practices designed to ensure that your personal information is appropriately protected. Please note that personal information may be transferred, accessed and stored globally as necessary in accordance with this privacy policy.

Oracle complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention when a customer and Oracle have agreed by contract that transfers of personal information from the European Economic Area (“EEA”) or Switzerland will be transferred and processed pursuant to the Privacy Shield for the relevant services. When conducting those activities on behalf of its EEA or Swiss customers, Oracle holds and/or processes personal information provided by the EEA or Swiss customer at the direction of the customer. Oracle will then be responsible for ensuring that third parties acting as an agent on our behalf do the same.

Oracle has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/list.

The following entities are covered entities under Oracle’s Privacy Shield self-certification: Delphi Asset Management Corporation; MICROS Fidelio Worldwide LLC; Oracle America, Inc.; Oracle Financial Services Software America, Inc.; Oracle Financial Services Software, Inc.; Oracle International Corporation; Oracle Taiwan LLC; Bronto Software, LLC; Monexa, LLC, NetSuite, Inc.; OrderMotion, Inc. With respect to personal information received or transferred pursuant to the Privacy Shield Framework, Oracle is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission and commits to cooperate with EU data protection authorities.

Dispute Resolution

If you have any complaints regarding our compliance with this privacy policy, you should first contact us. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with this privacy policy.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. Under certain conditions, more fully described on the Privacy Shield website, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Compliance

Oracle has appointed a Chief Privacy Officer. If you believe your services data has been used in a way that is not consistent with this policy, or if you have further questions related to this policy, please contact the Chief Privacy Officer through our inquiry form. Written inquiries may be addressed to:

Chief Privacy Officer, Oracle Corporation
10 Van de Graaff Drive