ORACLE

PROCESSOR CODE

(*Binding Corporate Rules* for the transfer of personal data
outside the EEA under Article 47 GDPR)

Introduction

Oracle provides cloud, consulting, technical support and other hosted, remote or on-premises computer-based information technology services to its Customers which may involve access to or storage of Personal Information of **Customer Individuals**. Oracle processes such Personal Information as a Processor on behalf of its Customers.

The Oracle Code of Ethics and Business Conduct express Oracle's commitment to strive to conduct our business in accordance with high ethical standards and in accordance with Applicable Law and Oracle policies, including with respect to the protection of Personal Information. This Processor Code (the **Processor Rules**) explains how Oracle will protect the Personal Information it processes on behalf of its Customers.

The Processor Rules constitute *Binding Corporate Rules* for the transfer of Personal Information to a third country outside the EEA under Article 47 GDPR and are legally binding and shall apply to and be enforced by Oracle and its Group Companies, including employees

These Processor Rules entered into force as of September 17, 2024 (**Effective Date**) and the parts of these Processor Rules relevant for Customer Individuals (including a list of the Group Companies that may be involved in Processing of Personal Information) will be published on the Oracle Internet site and will be made available to Customer Individuals and Customers upon request. Any questions concerning these Processor Rules may be directed to:

Oracle Privacy Office
Oracle Corporation
Chief Privacy Officer
Willis Tower
233 South Wacker Drive
45th Floor
Chicago, IL 60606
U.S.A.

The web form available here

Capitalized terms have the meaning set out in **Annex 1** (Definitions). Capitalized terms that are not defined in these Processor Rules have the meanings given to them in the GDPR.

Please refer to the following index for an overview of the content of these Processor Rules:

Article 1. Scope

These Processor Rules apply to the Processing of Personal Information by Oracle and its wholly or majority-owned affiliates (each a **Group Company**, collectively **Oracle**).

1.1 Scope

These Processor Rules address Oracle's worldwide Processing of Personal Information of individuals in the course of delivering services to its Customers (**Customer Individuals**). These Processor Rules apply to the Processing of Personal Information by electronic means and in systematically accessible paper-based filing systems.

These Processor Rules apply to the Processing by Oracle as a Processor of Personal Information in the course of delivering certain services to its Customers where such information is subject to a data transfer restriction under EEA Data Protection Laws and are Processed by Oracle outside of the EEA pursuant to a Services Contract that specially provides that these Processor Rules shall apply to such Personal Information.

In the Services Contract, Oracle and the Customer may also further agree on the scope of application of these Processor Rules.

Depending on the relevant Services, Oracle may Process the following categories of Personal Information:

(i) personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords;

(ii) 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;

(iii) 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;
(iv) financial details;
(v) goods and services provided;
(vi) unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

Depending on the relevant Services, Oracle may Process Personal Information related to the following categories of Customer Individuals:
(i) Customer representatives
(ii) Customer end users
(iii) Customer employees
(iv) Customer job applicants
(v) Customer contractors or partners
(vi) Customerend-customers and consumers

Oracle may supplement these Processor Rules through sub-policies and notices that are consistent with these Processor Rules.

Nothing in these Processor Rules will be construed to take away any rights and remedies that Customer Individuals may have under applicable local law. These Processor Rules provide supplemental rights and remedies to Customer Individuals only.

These Processor Rules shall be implemented within Oracle based on the timeframes specified in Article 8.

Article 2. Processing of Personal Information

Oracle Processes Personal Information for its Customers in the context of providing business services.

2.1 Role as Processor

In the context of providing certain business services (collectively, **Services**), Oracle may Process Personal Information as a Processor on behalf of Customers. Oracle will only Process such Personal Information on the basis of a validly entered into written or electronic agreement with a Customer (the **Services Contract**) which complies with EEA Data Protection Law to comply with any documented instructions, including regarding Transfers, received from the Customer, as needed to comply with Applicable Law, or for one or more of the following purposes:

(i) the provision of Oracle cloud services including:

(a) hosting, storage, backup, or archiving;

(b) maintenance and performance of systems and IT infrastructure (e.g., auditing use, managing servers);

(c) IT security purposes, including system resiliency and incident management;

(d) backup and disaster recovery;

(e) service change management;

(ii) the provision of Oracle technical support services including**:**

(a) providing technical assistance and product updates to Customers with regard to Oracle products, systems and services;

(b) life-cycle management of Oracle products, systems and services (e.g., planning, evaluation, demonstration, installation, calibration, maintenance, decommissioning) to facilitate continued and sustained use by a Customer of Oracle products, systems and services.

(iii) the provision of Oracle consulting services and advanced customer support services including:

(a) development and architecture services for the purpose of adjusting Oracle products, systems or services to meet a Customer's specifications (e.g., by engaging application specialists, undertaking project management activities, modifying of device or system);

(b) migration, implementation, configuration, consolidation, performance testing and tuning services;

(c) customer on-site support services for specific projects or on an ongoing basis;

(d) personalized and priority technical support services for critical customer systems and applications.

(iv) Oracle internal business and services process execution and management, including operation of the systems and networks these services run on, and which may involve incidental Processing of Personal Information for:

(a) internal auditing of Oracle Processor-related activities;

(b) activities related to compliance with Applicable Law ;

(c) use of de-identified, aggregate data to facilitate continuity, sustainability, service analysis and improvement of Oracle products and services.

2.2 Requests from Customers and Customer Individuals

Oracle will Process Personal Information in accordance with these Processor Rules Applicable Law, and will promptly and appropriately respond to Customers' inquiries relating to the Processing of Personal Information as well as to requests for assistance from a Customer as reasonably required to enable its compliance with its own obligations under EEA Data Protection Law (including assisting Customer in responding to investigations or inquiries by an EEA supervisory authority (**SA**) competent for the Customer regarding the Processing, all in accordance with the Services Contract.

If Oracle receives an inquiry, complaint, request or claim from a Customer Individual (a **Data Subject Request**) which expressly identifies the Customer and specifies that the Data Subject Request pertains to Personal Information that Customer provided to Oracle that relates to the Customer Individual, then Oracle will forward the Data Subject Request to the Customer without responding to the Customer Individual, unless agreed otherwise with the Customer. Oracle will execute appropriate technical and organizational measures, insofar as this is possible, when asked by the Customer, for the fulfilment of the Customer's corresponding obligations to respond to Data Subject Requests, including by communicating any useful information in order to help the Customer to comply with the duty to respect the rights of the Customer Individual under EEA Data Protection Law. If the Customer has disappeared factually or has ceased to exist in law or became insolvent, Oracle will handle the Customer Individual's request or complaint in accordance with Article 6.1.

Oracle shall immediately inform the Customer if, in its opinion, an instruction from the Customer infringes EEA Data Protection Law.

2.3 Termination of Services Contract

Upon termination of the Services Contract, Oracle will fulfill its obligations to the Customer with respect to Personal Information as provided in the Services Contract, including (for example) by allowing the Customer to retrieve such Personal Information via provided functionality.

When Oracle's obligations under the Services Contract have been fulfilled, Oracle will delete the Personal Information and, upon request of a Customer, will confirm that it has done so, except to the extent the Services Contract or Applicable Law provides otherwise. Thereafter, Oracle will no longer Process the Personal Information, except as authorized by the Services Contract (including the Processor Rules, as applicable) or as permitted by Applicable Law that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR.

Upon termination of the Services Contract, Oracle will allow its Processing facilities to be audited upon the Customer's request in accordance with Article 5.7 to verify that Oracle has complied with its termination-related obligations.

Article 3. Security and Confidentiality Requirements

Oracle takes appropriate measures to protect Personal Information from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access, and to provide notification in the event of a Data Security Breach.

3.1 Information Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Customer Individuals, Oracle shall take appropriate technical, physical and organizational measures to protect Personal Information from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

Oracle shall in any event implement and maintain the Corporate Security Pratices specified in the Services Contract and **Annex 4**, which may be revised by Oracle, provided that such changes do not materially diminish the level of security provided to the Personal Information Oracle Processes for its Customers.

3.2 Staff Access and Confidentiality

Staff shall be authorized to access Personal Information only to the extent necessary to: (i) perform the Processing as described in Article 2.1, and (ii) to perform their job. Oracle shall impose confidentiality obligations on Staff with access to Personal Information.

3.3 Data Security Breach Notification Requirement

Oracle shall notify the Customer of a Data Security Breach without undue delay after becoming aware that a Data Security Breach has occurred. Additional details regarding the reporting process and details regarding the Data Security Breach are specified in the Services Contract.

Article 4. Data Transfers to Third Parties or Internal Processors

Oracle may use subprocessors to Process Personal Information as provided in the Services Contract.

4.1 Subprocessor Contracts

Each Group Company may use third-party or internal subprocessors in the delivery of Services as authorized in the Services Contract. The Group Company will enter into a binding contract with any third-party subprocessor imposing data protection–related terms for the Personal Information that are no less protective than those imposed on such Group Company under the Services Contract and these Processor Rules. The Group Company entering into the Services Contract is referred to as the **Oracle Contracting Entity**. The Oracle Contracting Entity remains liable to the Customer for the performance of the contract by the subprocessors.

4.2 Publication of List of Subprocessors

Oracle shall publish and maintain on the appropriate Oracle website or online support portal lists of the internal or external subprocessors involved in the performance of the relevant Services. This overview shall be promptly updated in case of changes.

4.3 Notification of New Subprocessors and Right to Object

Oracle shall only engage external subprocessors for the delivery of the Services to Process Personal Information where there is a prior informed specific or general written authorization from the customer to do so. If a general authorization is given, the Customer will be informed by Oracle of any intended changes concerning the addition or replacement of subprocessors in a manner of their choosing and in such a timely fashion that the customer has the possibility to object to the involvement of such sub-processor in the delivery of the Services. In the event the objection is not unreasonable, Oracle and the Customer will work together in good faith to find a solution to address such objection, including but not limited to reviewing additional documentation supporting the subprocessors' compliance or making the Services available without the involvement of such processor. To the extent the parties cannot reach a mutually acceptable solution, the Customer shall have the right to terminate the relevant Services (i) in accordance with the terms of the Services Contract; (ii) without liability to Oracle or the Customer; and (iii) without relieving the Customer from its payment obligations under the Services Contract up to the date of termination.

Article 5. Accountability

These Processor Rules are binding on Oracle. The Responsibility Line of Business Executive shall be accountable for his/her business organization’s compliance with these Processor Rules. Oracle Staff must comply with these Processor Rules.

5.1 Role of Oracle EMEA

Oracle Corporation has tasked Oracle EMEA with the oversight, coordination and implementation of these Processor Rules.

5.2 Binding Effect

These Rules are legally binding on Oracle and shall apply to and be enforced by Oracle EMEA and its Group Companies, including Employees.

5.3 Privacy Governance

Oracle has implemented a global compliance organization to oversee and manage compliance with these Processor Rules as described in **Annex 2** (Privacy Governance Structure). The relevant Responsible Line of Business Executive is accountable for his/her business organization’s compliance with these Processor Rules. Where there is a question as to the applicability of these Processor Rules, Staff shall seek the advice of the appropriate Privacy Professional prior to the relevant Processing.

5.4 Policies and Procedures

These Processor Rules supplement all Oracle privacy policies, guidelines and notices that exist on the Effective Date. Oracle has developed and will continue to develop and implement policies and procedures to comply with these Processor Rules.

5.5 Staff Training

Oracle shall provide training on the obligations and principles laid down in these Processor Rules, and related confidentiality and security obligations, to Staff who have permanent or regular access to Personal Information or are involved in the development of tools used to Process Personal Information.

5.6 Records of Processing Activities

Oracle shall maintain Records of Processing Activities. A copy will be provided to the Competent SA upon request.

5.7 Monitoring and Audits

Oracle shall monitor and audit business processes and procedures that involve the Processing of Personal Information for compliance with these Processor Rules, and will allow for and contribute to Customer audits, in accordance with the procedures set forth in **Annex 3** (Procedures for Monitoring and Auditing Compliance).

Oracle shall take adequate measures to address violations of these Processor Rules identified during the monitoring or auditing of compliance pursuant to this Article.

5.8 Annual Privacy Report

The Chief Privacy Officer shall produce an annual Personal Information protection report for the General Counsel on Oracle's compliance with these Processor Rules, privacy protection risks and other relevant issues. Each Privacy Professional shall provide information relevant to the report to the Chief Privacy Officer .

5.9 Sanctions for Non-Compliance

Non-compliance of Staff with these Processor Rules may result in disciplinary action in accordance with Oracle policies and local law, up to and including termination of employment or contract.

5.10 Transfer Impact Assessment

Oracle will conduct a Transfer Impact Assessment prior to a Transfer of Personal Information under these Privacy Rules and maintain it for the duration of the Transfer.

Where a Transfer Impact Assessment shows (a) gap(s) in the protection for Customer Individuals under these Processor Rules, Oracle will promptly implement supplementary measures (e.g., contractual, technical or organisational measures to ensure security and confidentiality) including measures applied during transmission and to the Processing of the Personal Information in the country of destination to ensure compliance with these Processor Rules. Supplementary measures are not required in relation to laws and practices applicable to the Data Importer that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR.

The Transfer shall not take place or will be suspended where: (i) compliance with these Processor Rules cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent SA. In case of suspension, the Data Exporter may choose to terminate the Transfer.

The Data Importer shall– at the Data Exporter's option –return or delete the Personal Information that it received under these Processor Rules (including any copies thereof) and confirm to the Data Exporter that it has done so, where: (i) the Transfer has been suspended for a period longer than one calendar month, (ii) the Data Importer is in substantial or persistent breach of these Processor Rules, (iii) the Data Importer fails to comply with a binding decision of a Competent SA or court, or (iv) the Data Importer ceases to be bound by these Processor Rules. Until the Personal Information is deleted or returned, the Data Importer will continue to ensure compliance with these Privacy Rules and, if Applicable Law prevent the Data Importer from the return or deletion of Personal Information, the Data Importer will only process the Personal Information to the extent and for as long as required under Aplicable Law.

Oracle will conduct and document this assessment with the involvement of Oracle EMEA and the Global Privacy Office, and will notify the Data Exporter and Data Importer thereof. Oracle

EMEA and the Global Privacy Office will make the Transfer Impact Assessment available to all Group Companies, and to any Competent SA upon request.

Article 6. Complaints and Enforcement of Rights

These Processor Rules provide enforceable rights to Customer Individuals and Customers.

6.1 Enforcement Rights of Customer Individuals

If Oracle violates these Processor Rules with respect to its Processing of Personal Information of a Customer Individual (**Affected Individual**) the Affected Individual can, as a third-party beneficiary, enforce any claim against the Oracle Contracting Entity as a result of Oracle's breach of Articles 2, 3, 4.1, 4.2, 5.6, 6.1-6.3, 6.6, 6.7, 7.1, and 8.1.

6.2 Complaints

Affected Individuals are encouraged, but not required to file a written (including by email) complaint in respect of any claim they have under Article 6.1 with the Privacy Office via this form before filing any complaint or claim with a SA or court.

The Privacy Office shall be responsible for complaint handling. Each complaint will be assigned to an appropriate Staff member (either within the Privacy Office or within the applicable business unit or functional area). This Staff member will:

(i) promptly acknowledge receipt of the complaint;

(ii) analyze the complaint and, if needed, initiate an investigation;

(iii) If the complaint is well-founded, advise the applicable Privacy Professional so that a remediation plan can be developed and executed; and

(iv) maintain records of all complaints received, responses given, and remedial actions taken by Oracle.

Oracle will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Affected Individual within one calendar month of the date that the complaint was filed. The response shall be in writing and will be sent via the means that the Affected Individual originally used to contact Oracle (e.g., via mail or email), or such alternative means as agreed to by the Affected Individual. The response will outline the steps that Oracle has taken to investigate the complaint and will indicate Oracle's decision regarding what steps (if any) it will take as a result of the complaint.

In the event that Oracle cannot reasonably complete its investigation and response within four weeks, it shall inform the Affected Individual within one calendar month that the investigation is ongoing and that a response will be provided within the two calendar months following the original one month period.

If Oracle's response to the complaint is unsatisfactory to the Affected Individual (e.g., the request is denied without providing an adequate justification) or Oracle does not observe the conditions of the complaints procedure set out in this Article 6.1, the Affected Individual can file a complaint with the Privacy Officer or a complaint or claim with the authorities or the courts in accordance with Article 6.3.

6.3 Where Complaints or Claims May be Filed

The Affected Individual may, at his or her choice, submit a complaint or a claim under Article 6.2 to:

(i) The Lead SA or the courts in Ireland, against Oracle EMEA;

(ii) The SA in the EEA Country where (a) the Affected Individual has his or her habitual residence or place of work or (b) the infringement took place, against the Oracle Contracting Entity or Oracle EMEA; or

(iii) The courts in the EEA Country (a) where the Affected Individual has his or her habitual residence, or (b) of origin of a Transfer under these Processor Rules, against the Oracle Contracting Entity instead or Oracle EMEA;

Oracle accepts liability, and accepts to pay compensation in accordance with Article 6.4, for a violation by a subprocessor (whether another Group Company or a third-party subprocessor) of its obligations, although Oracle may assert any defense that such subprocessor could have asserted.

The SAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Affected Individual will not prejudice the substantive or procedural rights he or she may have under Applicable Law.

6.4 Right of Customer Individuals to Claim Damages

In case an Affected Individual has a claim under Article 6.2, such Affected Individual shall be entitled to recover damages suffered by that Affected Individual resulting from a violation of these Processor Rules to the extent provided by applicable EEA law.

To bring a claim for damages, the Affected Individual must demonstrate that he or she has suffered the relevant damages and to establish facts which show it is plausible that the damage has occurred because of a violation of these Processor Rules. Oracle must then prove that the damages suffered by such Affected Individual are not attributable to Oracle or a subprocessor or assert other applicable defenses.

Oracle may not rely on a breach by a Group Company or subprocessor of its obligations to avoid liability except to the extent a defense of such Group Company or subprocessor would also constitute a defense of Oracle. Oracle may, however, assert any defenses or rights that would have been available to the Customer. Oracle also may assert any defenses that Oracle could have asserted against the Customer (such as contributory negligence), in defending against the Affected Individual’s claim.

6.5 Rights of Customers

The Customer may enforce these Processor Rules against the Oracle Contracting Entity or, if the Oracle Contracting Entity is not established in an EEA Country, against Oracle EMEA. Oracle EMEA shall ensure that adequate steps are taken to address violations of these Processor Rules by the Oracle Contracting Entity or any other Group Company.

The Oracle Contracting Entity or Oracle EMEA may not rely on a breach by another Group Company or a subprocessor of its obligations to avoid liability, except to the extent a defense of such Group Company or Sub-Processor would also constitute a defense of Oracle.

In case of a violation of these Processor Rules, and where the Customer demonstrated ist has suffered damages and establishes facts which show that it is likely that damage has occurred because of a violation of these Processor Rules, the Customers shall be entitled to compensation of damages consistent with the Services Contract.

6.6 Mutual Assistance and Redress

All Group Companies shall co-operate and assist each other to achieve compliance with these Processor Rules, including an audit or inquiry by the Lead SA, the Customer or a Customer SA.

The Group Company that receives a request, complaint or claim is responsible for promptly notifying and informing the Privacy Office thereof and handling any communication with such Customer Individual regarding his or her request, complaint or claim as instructed by the Privacy Office, except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse Oracle EMEA.

6.7 Advice of the SAs

Oracle shall cooperate with and take into account and abide by the advice of the Lead SA and Competent SA, issued on the interpretation and application of these Processor Rules.

6.8 Responsibility for Damages by Controller and Processor

Where Oracle and the Customer are involved in the same Processing of Personal Information and are found to be responsible for any damage caused by such Processing, the Affected Individual shall be entitled to receive compensation for the entire damage directly from Oracle, unless Oracle proves that it is not responsible for the event giving rise to the damage suffered by the Affected Individual. If, under this Article, Oracle pays full compensation, it shall be entitled to claim back from the Controller the part of the compensation corresponding to the Customer’s part of responsibility for the damage.

6.9 Law Applicable to these Processor Rules

These Processor Rules shall be governed by and interpreted in accordance with Irish law.

Article 7. Conflicts and Notification Duties to SAs

7.1 Conflict Between these Processor Rules and Local Law

Each Group Company shall monitor its Applicable Law and practices and, if it becomes aware that it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with these Processor Rules or that have a substantial effect on the protection offered by these Processor Rules (including any Transfer Impact Assessments performed thereunder), the relevant Responsible Line of Business Executive shall promptly consult with the Global Privacy Office to determine how to comply with these Processor Rules and address the conflict, including by implementing additional appropriate safeguards in accordance with

Article 5.10. The Global Privacy Office may seek the advice of the Lead SA and/or Competent SA.

If any Group Company determines that it is unable to comply with its processor obligations under these Processor Rules or becomes aware that Applicable Law or practice of a Third Country or an instruction of a Customer, is likely to have a substantial adverse effect on Oracle's ability to meet its obligations with respect to the Processing of Personal Information, Oracle will promptly report this to Oracle EMEA, the Competent SA, and the affected Customer, and will coordinate with the affected Customer to report this to the Customer's SA. The affected Customer will have the right to suspend the relevant Transfer until such time the Processing is adjusted in such a manner that the non-compliance is remedied. To the extent such adjustment is not possible, the Customer will have the right to terminate the relevant part of the Processing by Oracle in accordance with the terms of the Services Contract.

7.2 Requests for Disclosure of Personal Information

If Oracle receives a Disclosure Request it will first assess the legality thereof, in particular, whether it remains within the powers granted to the requesting authority. Oracle will challenge Disclosure Requests that it considers unlawful under the laws of the Third Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, Oracle shall seek interim measures with a view to suspending the effects of the Disclosure Request until the requesting authority has decided on its merits. Oracle shall not disclose the Personal Information requested until required to do so under the applicable procedural rules and will only provide the Personal Information that is strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. Oracle will document this assessment and provide it to the Data Exporter and, upon request, to the Competent SA.

Subject to this paragraph, Oracle shall inform the Customer and the Lead SA, and cooperate with the Customer to inform the Customer's SA, of a Disclosure Request. Oracle will also request that the requesting authority delay the Disclosure Request in order to enable the Lead SA and/or the Customer's SA to issue an opinion on the validity of the relevant disclosure. Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure.

If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Oracle will request the relevant authority to waive this prohibition and will document that it has made this request, which documentation will be provided to the Lead SA upon request. If, despite its efforts, Oracle does not obtain a waiver, Oracle will on an annual basis provide to the Lead SA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by Applicable Law.

In any event, any transfers by Oracle of Personal Information in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

This Article does not apply to requests received by Oracle from other government agencies in the normal course of its activities, which Oracle can continue to provide in accordance with Applicable Law, as far as the request is necessary and proportionate in a democratic society to protect one of the objectives listed in article 23(1) of the GDPR.

Article 8. Adoption and Modification of these Processor Rules

Oracle has adopted these Processor Rules and any changes will be made in accordance with the procedure set forth in these Processor Rules.

8.1 Effective Date

These Processor Rules have been adopted by Oracle and will enter into force as of [•] (**Effective Date**). The Processor Rules will be published on the Oracle corporate Internet site and are made available to Customer Individuals and Customers upon request.

8.2 Changes

Any changes to these Processor Rules require the prior approval of the General Counsel and shall thereafter be communicated to the Group Companies without undue delay.

(i) **Effective Time of Changes**

Any change shall enter into force with immediate effect after it is approved and published on the Oracle Internet site.

(ii) **Prior Versions**

Any request, complaint or claim of a Customer Individual involving these Processor Rules shall be judged against the version of these Processor Rules that are in force at the time the request, complaint or claim is made.

(iii) **Reporting of Changes**

The Chief Privacy Officer keeps a fully updated list of Group Companies bound by these Processor Rules and records any updates to the Processor Rules and provides the necessary information to the Lead SA or Competent SA upon request. The Chief Privacy Officer shall promptly inform the Lead SA of changes to these Processor Rules that significantly affect the protection offered by these Processor Rules or these Processor Rules itself and will be responsible for and coordinating Oracle’s responses to questions of the Lead SA in respect thereof. Other changes to these Processor Rules (if any) will be notified by the Chief Privacy Officer to the Lead SA on a yearly basis, including a brief explanation of the reasons justifying the update.

Where a change to these Processor Rules has a significant impact on the Processing conditions of the Customer Services, Oracle will promptly inform the Lead SA thereof including a brief explanation for such change as well as provide notice of such change to the Customer. Within 30 days of receiving such notice, the Customer may object to such change by providing written notice to Oracle. In the event that the parties cannot reach a mutually acceptable solution, Oracle shall put in place an alternative data transfer solution. In the event no alternative data transfer solution can be put in place, the Customer will have the right to suspend the relevant transfer of Personal Information to Oracle. In the event a suspension of the relevant data transfers is not possible, Oracle shall enable the Customer to terminate the relevant Customer Services in accordance with the terms of the Services Contract.

8.3 Transition Periods

(i) **Transition Period for New Group Companies**

Any entity that becomes a Group Company after the Effective Date shall comply with these Processor Rules within two years of becoming a Group Company. During this transition period, no Personal Information will be Transferred under these Processor Rules until the relevant Group Company has achieved compliance with these Processor Rules.

(ii) **Transition Period for Divested Entities**

A Divested Entity (or specific parts thereof) will remain covered by these Processor Rules after its divestment for such period as is required by Oracle to disentangle the Processing of Personal Information relating to such Divested Entity.

(iii) **Transition Period for Existing Agreements**

Where there are existing agreements with Third Parties that are affected by these Processor Rules, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Annexes	
Annex 1	Definitions
Annex 2	Privacy Governance Structure
Annex 3	Procedures for Auditing and Monitoring Compliance
Annex 4	Oracle Corporate Security Practices

ANNEX 1 - DEFINITIONS

ADEQUACY DECISION shall mean a decision issued by the European Commission under EEA Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.

AFFECTED INDIVIDUAL shall mean the individual referred to in Article 11.1.

APPLICABLE LAW shall mean any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (including any and all legislative and/or regulatory amendments or successors), to which a Group Company is subject.

ARTICLE shall mean an Article in these Processor Rules.

COMPETENT SA shall mean the SA competent to audit under Article 3 of Annex 3.

CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Information.

COUNTRY shall mean each country in which a Group Company is established.

CUSTOMER shall mean the customer who has entered into a contract with Oracle for the delivery of Oracle Services and is the Controller for the Processing of Personal Information. .

CUSTOMER INDIVIDUAL shall mean any individual whose Personal Information is Processed by Oracle in its role as a Processor in the course of delivering Oracle Services to a Customer.

DATA EXPORTER shall mean the Group Company that transfers Personal Information under these Rules.

DATA IMPORTER shall mean the Group Company that is the recipient of a transfer of Personal Information under these Rules.

DATA SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted customer content (including Personal Information) that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Customer Individual. A Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Information by an Employee of Oracle or Third Party subprocessor or an individual acting under their respective authority, if

- the acquisition, access, or use of Personal Information was in good faith and within the course and scope of the employment or professional relationship of such Employee or other individual; and
- the Personal Information is not further acquired, accessed, used or disclosed by any person.

DISCLOSURE REQUEST shall mean a legally binding request for disclosure of (or direct access to) Personal Information from a law enforcement authority or state security body of a Third Country.

DIVESTED ENTITY shall mean the divestment by Oracle of a Group Company or business by means of:
- a sale of shares that results in the divested Group Company no longer qualifying as a Group Company; and/or
- a demerger, sale of assets, or any other manner or form.

EEA COUNTRIES shall mean the countries in the EEA.

EEA DATA PROTECTION LAW shall mean the provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.

EEA or **EUROPEAN ECONOMIC AREA** shall mean all Member States of the European Union, Norway, Iceland and Liechtenstein and, for the purposes of these Processor Rules, Switzerland. Oracle's General Counsel can decide to include other countries in this definition, provided that such country is subject to an Adequacy Decision.

EFFECTIVE DATE shall mean the date on which these Processor Rules become effective as set forth in Article 8.1.

EMPLOYEE shall mean an employee, job applicant or former employee of Oracle. This term does not include people working at Oracleas consultants or employees of Third Parties providing services to Oracle.

GDPR shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

GENERAL COUNSEL shall mean the General Counsel of Oracle Corporation.

CHIEF PRIVACY OFFICER shall mean the officer as referred to in Article 1 of **Annex 2**.

GROUP COMPANY shall mean Oracle Corporation and any company or legal entity of which Oracle Corporation, directly or indirectly owns more than 50% of the issued share capital.

INTERNAL PROCESSOR shall mean any Group Company that Processes Personal Information on behalf of another Group Cafompany.

LEAD SA shall mean the SA of Ireland.

ORACLE shall mean Oracle Corporation and its Group Companies.

ORACLE CONTRACTING ENTITY shall mean the Oracle Group Company that has entered into a Services Contract for the provision of Services.

ORACLE CORPORATION shall mean Oracle Corporation, incorporated in the State of Delaware, and having its its principle place of business in the State of California, United States.

ORACLE EMEA shall mean Oracle EMEA Limited, having its registered seat in Dublin, Ireland.

PERSONAL INFORMATION shall mean any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), insofar as this information relates to an individual and is Processed by Oracle.

PRIVACY PROFESSIONAL shall mean the privacy professionals appointed by the Chief Privacy Officer pursuant to **Annex 2**.

PROCESSING shall mean any operation that is performed on Personal Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Information.

RECORDS OF PROCESSING ACTIVITIES shall mean a record of Processing activities maintained in writing, including in electronic form, by Oracle that contains the following information:

a. the name and contact details of the Group Company that is the Controller;

b. the Processing Purposes;

c. the categories of Personal Information;

d. the categories of recipients to whom Personal Information have been disclosed;

e. where applicable, information about transfers of Personal Information to a country not subject to an Adequacy Decision;

f. where possible, the envisaged retention periods; and

g. where possible, a general description of the measures under Article 3.1.

REGION shall mean a particular geographic area in which certain Countries are grouped.

RESPONSIBLE LINE OF BUSINESS EXECUTIVE shall mean the lowest-level Oracle line of business executive or the non-executive general manager of an Oracle ORU (Organizational Reporting Unit) who has primary budgetary ownership of the relevant Processing.

SA shall mean any supervisory authority of one of the EEA Countries.

SERVICES shall mean the services listed in Article 2.1 as contracted by the Customer under the Services Contract

SERVICES CONTRACT shall mean a written or electronic agreement with a Customer.

STAFF shall mean all Employees and other persons who Process Personal Information as part of their respective duties or responsibilities using Oracle information technology systems or working primarily from Oracle premises.

THIRD COUNTRY shall mean a country outside the EEA to which Personal Information is transferred, where such transfer is not covered by an Adequacy Decision.

THIRD PARTY shall mean any person or entity (e.g., an organization or government authority) outside Oracle or a Customer.

TRANSFER shall mean a transfer (or set of transfers), including disclosure of, or remote access to, Personal Information under these Processor Rules to a Group Company in a Third Country.

TRANSFER IMPACT ASSESSMENT shall mean an assessment on whether, taking into account the specific circumstances of the Transfer, the laws and practices of the Third Country, including those requiring the disclosure of Personal Information to public authorities or authorizing access by such authorities, prevent Oracle from fulfilling its obligations under these Processor Rules.

In assessing the laws and practices of the Third Country, Oracle shall take into account in particular:

a. the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Third Country or to another Third Country, including:
   i. purposes for which the data are Transferred and Processed (e.g. marketing, HR, storage, IT support);
   ii. types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
   iii. sector in which the Transfers occur;
   iv. categories and format of the Personal Information Transferred;
   v. location of the Processing including storage;
   vi. transmission channels used.

b. the laws and practices of the Third Country relevant in light of the circumstances of the Transfers, including requirements to disclose Personal Information to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Personal Information during transit between the country of the Data Exporter and the Third Country;

c. any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under these Processor Rules, including measures applied during transmission and to the Processing of Personal Information in the Third Country.

INTERPRETATION OF THESE PROCESSOR RULES:

- Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;
- headings are included for convenience only and are not to be used in construing any provision of these Processor Rules;
- if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- the male form shall include the female form;
- the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;
- a reference to a document (including, without limitation, a reference to these Processor Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Processor Rules or that other document; and
- a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2 - PRIVACY GOVERNANCE STRUCTURE

1. Chief Privacy Officer

Oracle Corporation shall appoint a Chief Privacy Officer who benefits from the support of Oracle management and is responsible for:

(i) Developing, reviewing and updating Oracle’s privacy policies, procedures, system information and training an awareness programs (as required by Article 5);

(ii) Supervising and ensuring compliance with these Processor Rules;

(iii) Providing the annual report (as required by Article 5.8) and periodic reports, as appropriate, to Oracle’s General Counsel on data protection risks and compliance issues as described in Article 4 of **Annex 3**; overseeing the collection, investigation and resolution of privacy inquiries, concerns and complaints;

(iv) Coordinating, in conjunction with the appropriate Privacy Professionals, official investigations or inquiries into the Processing of Customer Personal Information by a public authority;

(v) Determining and updating appropriate sanctions for violations of these Processor Rules (e.g., disciplinary standards) in co-operation with other relevant internal functions, such as HR and Legal.

(vi) Advising in respect of conflicts between these Processor Rules and Applicable Law as described in Article 7.1 of the Processor Rules;

(vii) Maintaining a fully updated list of the Group Companies and Third Party subprocessors, and keep track and records of updates to these Processor Rules.

2. Privacy Office

The Chief Privacy Officer has established and heads Oracle’s Privacy Office, consisting of a global network of Privacy Professionals sufficient to direct compliance with these Processor Rules within their respective regions or countries. Oracle has appointed a data protection officer for the EEA (**DPO**). The DPO performs his/her statutory duties under EEA Data Protection Law and works with the Chief Privacy Officer to advise and assist upon compliance with these Processor Rules and functions as the contact person for the SAs. The DPO reports on privacy compliance to the highest management level of Oracle EMEA.

The Privacy Office performs at least the following tasks:

(i) Regularly advising the global Oracle organization and other relevant internal functions (e.g., Marketing, HR, Development, Sales) on privacy risks and compliance issues;

(ii) Ensuring that the Responsible Line of Business Executives maintain an inventory of the system information for all systems and processes that Process Personal Information (as required by Article 5.6);

(iii) Implementing the privacy compliance framework (as developed by the Privacy Office in accordance with Article 5);

(iv) Making itself available for requests for privacy approvals or advice;

(v) Handling privacy requests and complaints;

(vi) Owning and authorizing all appropriate privacy sub-policies in their regions or countries; and

(vii) Cooperating with the relevant internal functions, including legal, information security, operations and development.

3. Responsible Line of Business Executive

The Responsible Line of Business Executive shall perform at least the following tasks:

(i) Ensuring that the policies and procedures are implemented and the system information is maintained (as required by Article 5);

(ii) Maintaining (or ensuring access to) an inventory of the system information for all systems and processes that Process Personal Information and providing such system information to the Privacy Office as required for the Privacy Oddice to comply with tasks listed in Article 2 sub (ii) of this Annex;

(iii) Ensuring that Personal Information is returned or securely deleted upon termination of the Services Contract (as required by Article 2.3);

(iv) Consulting with the Privacy Office whenever there is a conflict between the Processor Rules and Applicable Law (as required by Article 7.1);

(v) Informing the Privacy Office of any new legal requirement that the Responsible Line of Business Executive believes to interfere with Oracle’s ability to comply with these Processor Rules (as required by Article 7.1).

4. Privacy Professionals with statutory position

Where a Privacy Professional holds his/her position pursuant to law, he/she shall carry out his/her job responsibilities to the extent they do not conflict with his/her statutory position..

ANNEX 3 - PROCEDURES FOR MONITORING AND AUDITING COMPLIANCE

1. Internal Audits

Oracle’s Business Assessment and Audit (**BA&A**) organization shall audit business processes and procedures that involve the Processing of Personal Information for compliance with all aspects of these Processor Rules, including methods of ensuring that corrective actions will take place. The audits shall be carried out in the course of the regular activities of BA&A organization or at the request of the Chief Privacy Officer or the General Counsel. The Chief Privacy Officer may request to have an audit as specified in this Article conducted by an accredited external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer , the General Counsel and the Privacy Office shall be informed of the results of the audits. Any violations of the Processor Rules will be reported to the Responsible Line of Business Executive and to the board of directors of Oracle. A copy of the audit results related to compliance with these Processor Rules will be provided upon request to the Lead SA or Competent SA for Oracle, and the Customer or the Customer’s SA.

2. Customer Audit

Oracle shall, at its option, either

(i) Allow for, and contribute to, an audit by the Customer by making available the data center facilities or systems it uses for the Processing of Personal Information for an audit by the Customer or a qualified independent third party auditor selected by the Customer, provided such auditor (a) is reasonably acceptable to Oracle, and (b) has executed a written confidentiality agreement reasonably acceptable to Oracle before conducting the audit. In accordance with the audit provisions of the applicable Services Contract, audits shall be conducted no more than once per year and during regular business hours, and shall be subject to (a) a written request submitted to Oracle at least two weeks in advance of the proposed audit date, (b) a detailed written audit plan reviewed and approved by Oracle and (c) Oracle’s on-site health and safety or other relevant security policies. Upon completion of the audit, the Customer shall provide Oracle with a copy of the audit report, which shall be treated as confidential information pursuant to the terms of the Services Contract.

(ii) Provide to the Customer a statement issued by a qualified independent third party assessor certifying that the Oracle business processes and procedures that involve the Processing of Personal Information comply with the principles set forth in these Processor Rules.

3. SA Audit

The Lead SA may request an audit of the facilities used by Oracle for the Processing of Personal Information for compliance with these Processor Rules.

In addition, the SA of the EEA country at the origin of transfer under these Rules will be authorized to audit the relevant transfer for compliance with these Processor Rules. Oracle will accept and co-operate with such audits.

4. Annual Report

The Chief Privacy Officer shall produce an annual Personal Information protection report for the General Counsel on Oracle's compliance with these Processor Rules, privacy protection risks, and other relevant issues.

Each Privacy Professional shall provide information relevant to the annual privacy report to the Chief Privacy Officer .

5. Mitigation

Oracle shall, if so indicated, ensure that adequate steps are taken to address breaches of these Processor Rules identified during the monitoring or auditing of compliance pursuant to this Annex 3.

ANNEX 4 – ORACLE CORPORATE SECURITY PRACTICES

Please note: in this Annex 4, references to "you" should be read as references to "the Customer".

INTRODUCTION

Oracle's mission is to help people see data in new ways, discover insights and unlock endless possibilities.
Oracle's security practices reflect the various ways Oracle engages with its customers:

- Oracle Corporate Security programs, policies and recommendations guide the IT teams managing Oracle's corporate network and systems as well as guiding the operational, cloud and services Lines of Business.
- In this document, "customer data" means any data stored in a customer's computer system (data accessed by or provided to Oracle while performing services for a customer) or data in a customer's cloud tenancy.
- Third parties provided access to customer data by Oracle ("subprocessors") are required to contractually commit to materially equivalent security practices.

Oracle continually works to strengthen and improve the security controls and practices for internal operations and services offered to customers. These practices are subject to change at Oracle's discretion.
Companies that Oracle acquires are required to align with these security practices as part of the integration process. This duration and outcome of each aspect of the integration process relies on the size, complexity, contractual commitments and regulatory requirements applicable to the acquired company's products, services, personnel and operations.

Oracle's Cloud, Support, and Services lines of business have developed statements of security practices that apply to the respective service offerings. These are published and incorporated into applicable orders.

The purpose of this paper is to summarize key Oracle's security practices and programs. This paper does not exhaustively describe all security practices and programs which may be applicable and relevant to individual Lines of Business, products or services.

ORACLE CORPORATE SECURITY

Oracle's Corporate Security Programs are designed to protect both Oracle and customer data, such as:

- Mission-critical systems that customers rely upon for cloud, technical support and other services
- Oracle source code and other sensitive data against theft and malicious alteration
- Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle's internal IT systems

Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are generally aligned with the ISO/IEC 27002:2022 and ISO/IEC 27001:2022 standards and guide security within Oracle.

Reflecting the recommended practices in security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective and corrective security controls with the objective of protecting information assets.

ORGANIZATIONAL SECURITY

Oracle’s overarching Organizational Security is described in the Oracle security organization policy and the Oracle information security policy.

The Chief Corporate Architect is one of the directors of the Oracle Security Oversight Committee. The Chief Corporate Architect manages the Corporate Security departments which guide security at Oracle. These departments manage the corporate security programs, define corporate security policies, and provide global oversight for Oracle’s security policies and requirements.

Oracle Security Oversight Committee

The Oracle Security Oversight Committee (OSOC) oversees the implementation of Oracle-wide security programs, including security policies and data privacy standards. The OSOC is chaired by Oracle’s CEO, General Counsel, and Chief Corporate Architect.

Corporate Security Organizations

Global Information Security

Global Information Security (GIS) defines policies for the management of information security across Oracle. GIS provides direction and advice to help Lines of Business (LoBs) protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle.

Global Product Security

The Global Product Security organization acts as a central resource to help Oracle development teams improve the security of Oracle products. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products.

Under the leadership of Oracle’s Chief Security Officer, Global Product Security promotes the use of Oracle Software Security Assurance standards throughout Oracle, acts as a central resource to help development teams improve the security of their products, and handles specialized security functions.

Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing physical security for the protection of Oracle’s employees, facilities, business enterprise, and assets. Oracle’s physical security standards and policies have been developed to generally align with several physical security industry initiatives, including the International Organization for Standardization (ISO), United States Customs Trade Partnership Against Terrorism (CTPAT), American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, and the Payment Card Industry Security Standards Council. Physical security controls are described later in this document.

Corporate Security Architecture

The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle’s IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's information security goals. The corporate security architect works with Global

Information Security and Global Product Security, and the Development Security Leads to develop, communicate and implement secure architectures.

Corporate Security Architecture (CSA) manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud and all other lines of business.

Global Trade Compliance

Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance and enforcement to enable worldwide trade compliant business processes across Oracle in order to uphold and protect Oracle's global trade privileges. GTC manages Oracle's global trade compliance portfolio and is responsible for global trade regulatory interpretation and coordination of policy advocacy, Global Brand Protection, Hardware Compliance Strategy and Market Access programs. Further, GTC reviews and resolves global trade compliance matters; serves as the clearinghouse for all global trade compliance information, including product classification, and is empowered to take actions necessary to ensure Oracle remains compliant with U.S. and applicable local Customs, import, and export laws, regulations and statutes.

Line of Business Security Organizations

Lines of Business (LoB) have security teams which oversee their products, systems and cloud services managed by that organization. LoBs are required to define technical standards in accordance with Oracle’s information security policies, as well as drive compliance to Oracle policies and standards within their organization and cloud service teams. LoBs are also required to comply with Corporate Security program requirements and directions. This paper does not describe LoB’s specific security organizations, standards, and programs.

Oracle Information Technology Organizations

Oracle information technology (IT) and cloud DevOps organizations are responsible for IT security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation and security technical assessment for new infrastructure.

Independent Review of Information Security

Oracle’s Business Assessment & Audit is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle’s Lines of Business.

PRIVACY

The Oracle General Privacy Policy addresses information we collect in connection with your use of Oracle websites, mobile applications, and social media pages that link to the General Privacy Policy, your interactions with Oracle during in-person meetings at Oracle facilities or at Oracle events, and in the context of other online or offline sales and marketing activities.

The Services Privacy Policy describes our privacy and security practices that apply when handling (i) services personal information in order to perform Consulting, Technical Support, Cloud and other services on behalf of Oracle customers; and (ii) personal information contained in systems operation data generated by the interaction of (end-)users of these services with Oracle systems and networks. Oracle Advertising Privacy Policy (also referred to as the ‘Privacy Policy’ or the ‘Oracle Data Cloud Privacy Policy’) informs consumers on the collection, use, sharing, and selling (collectively referred to as ‘processing’) of your personal information in connection with Oracle’s provision of Oracle Advertising services designed to help Oracle’s customers’ and partners’ online and offline marketing activities (‘Oracle Advertising’). This policy also explains your privacy rights in relation to these processing activities.

CUSTOMER DATA PROTECTION

Oracle’s media sanitation and disposal policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required against unauthorized retrieval and data reconstruction. Electronic storage media include laptops, hard drives, storage devices and removable media.

ASSET CLASSIFICATION AND CONTROL

Responsibility, Inventory, and Ownership of Assets

Oracle’s formal information protection policy provides guidelines for all Oracle information classification and minimum handling requirements for each classification.
Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle’s information systems asset inventory policy requires that Lines of Business (LoBs) mantain accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services.

Asset Classification and Control

Oracle categorizes information into four classes—Public, Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data:

- “Public” information is not sensitive, and there is no need with it remaining confidential to Oracle.
- “Oracle Internal” information must remain confidential to Oracle.
- “Oracle Restricted” and “Oracle Highly Restricted” information must remain confidential to Oracle and access within Oracle must be restricted on a “need to know” basis, with additional handling requirements for “Oracle Highly Restricted” information.

Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Retention of customer data in cloud services is controlled by the customer and is subject to terms in their contract.

Customer data is classified under one of Oracle's top two categories of confidential information for the purpose of placing limits on access, distribution and handling of such data. Oracle keeps the information confidential in accordance with the terms of customer’s order.

HUMAN RESOURCES SECURITY

Oracle places a strong emphasis on personnel security. The company maintains ongoing initiatives intended to help minimize risks associated with human error, theft, fraud and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.
Employees who fail to comply with Oracle policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

Employee Screening

In the United States, Oracle currently uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations and local Oracle policy.

Confidentiality Agreements

Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.

Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters and security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers privacy principles and data handling practices required by company policy.

PHYSICAL SECURITY

Oracle Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle's employees, facilities, business enterprise, and assets.
Oracle currently has implemented the following protocols in Oracle facilities:

- Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.
- Visitors are required to sign a visitor's register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle.
- Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle's employment must return keys/cards and key/cards are deactivated upon termination.
- Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.
- Mixture of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of physical security events.
- Centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as per Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws.

OPERATIONS MANAGEMENT

Protection Against Malicious Code

Oracle policy requires the use of antivirus protection and firewall software on endpoint devices such as laptops, desktops and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.
The Oracle information technology organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. They are responsible for:

- notifying internal Oracle system users of both any credible virus threats and when security updates are available
- providing automation to manage and verify antivirus configuration

Employees are prohibited from altering, disabling or removing antivirus software and the security update service from any computer. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.

Monitoring and Protection of Audit Log Information

Oracle logs certain security-related activities on operating systems, applications, databases and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events and/or logs being overwritten.

Oracle reviews logs for security event investigation and forensic purposes. Identified anomalous activities feed into security event management processes. Access to security logs is provided on the basis of need-to-know and least privilege. Where available for cloud services, log files are protected by strong cryptography and other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

Network Controls

Oracle has implemented and maintains strong network controls for the protection and control of both Oracle and customer data during its transmission. Oracle's network security policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated. For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measures defined by Global Physical Security (GPS).

Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use approved virtual private networks (VPNs). Corporate systems available outside the corporate network are protected by alternative security controls such as multifactor authentication.

Oracle's network security policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.
Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle's third-party network access policy.

ACCESS CONTROL

Access control refers to the policies, procedures and tools that govern access to and use of resources. Examples of resources include a physical server, file, application, data in a database and network device.

- Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.
- Default-deny is a network-oriented configuration approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.

Oracle's logical access control policy is applicable to access control decisions for all Oracle employees and any information-processing facility for which Oracle has administrative authority. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability and auditing functionality. This policy does not apply to customer end user accounts for Oracle cloud services.

User Access Management

Oracle user access is provisioned through an account provisioning system that is integrated with Oracle's Human Resources database. Access privileges are granted based on job roles and require management approval. Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, database administrators, system administrators, and network engineers.

Privilege Management

Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval and review of access are based on the following principles:

- Need to know: Does the user require this access for his job function?
- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

Password Management

The use of passwords is addressed in the Oracle password policy. Oracle has strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt.

Employees must keep their passwords confidential and secured at all times and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Oracle system or applications passwords for non-Oracle applications or systems.

Periodic Review of Access Rights

Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony and physical access.

INFORMATION SYSTEMS DEVELOPMENT, AND MAINTENANCE

Technical Vulnerability Management

Oracle has formal practices designed to identify, analyze, and remediate the technical security vulnerabilities that may affect our enterprise systems and your Oracle Cloud environment.
The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internal and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments.

Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud is to remediate these issues according to their severity and the potential impact. The Common Vulnerability Scoring System (CVSS) is one of the criteria used in assessing the relative severity of vulnerabilities and their potential impact. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system.
Oracle aims to complete all cloud remediation activities, including testing, implementation, and reboot (if required) within planned maintenance windows. Emergency maintenance will be performed as described in the Oracle Cloud Hosting and Delivery Policies and applicable Pillar documentation.

Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Customers and security researchers can report suspected security vulnerabilities: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system.

INFORMATION SECURITY INCIDENT RESPONSE

A security incident is a security event that Oracle, per its incident response process, has determined results in the actual or potential loss of confidentiality, integrity, or availability of Oracle managed assets (systems and data). Oracle will respond to information security events when Oracle suspects unauthorized access to Oracle-managed assets. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logging.

Security Incident Policy and Operations

Oracle's Security Incident Management Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction for security event and incident preparation, detection, investigation, resolution and forensic evidence handling across Oracle's Lines of Business (LoB). This policy does not apply to availability issues (outages) or to physical security events.

Global Information Security further defines roles and responsibilities for the incident response teams within the LoBs. All LoBs must comply with Global Information Security guidance for managing information security events and implementing timely corrective actions.

Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. LoB incident response teams, as required by the Security Incident Management Policy, conduct post-event analysis to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Oracle can support legally admissible forensic data collection when necessary.

Notifications

If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts, suspected incidents and incident history are not shared externally.

ORACLE SOFTWARE SECURITY ASSURANCE

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing and maintenance of its products, whether they are used on-premises by customers or delivered through Oracle cloud services.

Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience. Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

- **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the cloud.
- **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups and the use of automated analysis and testing tools.
- **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

Coding Standards & Security Training

Developing secure software requires consistently applied methodologies across the organization; methodologies that conform to stated policies, objectives, and principles. Oracle's objective is to produce secure code. To that end, Oracle requires that all of development abide by secure coding principles that are documented and maintained to remain relevant. Developers must be familiar with these standards and apply them when designing and building Oracle products.

Oracle Secure Coding Standards and related guidance have evolved and expanded over time to encompass emerging technologies such as Artificial Intelligence and Machine Learning (AI/ML) and address the most common issues affecting Oracle code, new threats as they are discovered, and new customer use cases for Oracle technology.

All Oracle staff are required to take security training. Technical development staff, up to and including vice presidents, who are involved in building, maintaining, customizing or testing product code are required to take an OSSA awareness course.

Additionally, Oracle adapted its secure coding principles and created training material for use by its consulting and services organizations when they are engaged in producing code on behalf of customers.

Security Analysis & Testing

Oracle requires that security testing be performed for its on-premises and cloud products. Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to support comprehensive security testing coverage of Oracle products.

Functional security testing is typically executed by regular product Quality Assurance (QA) teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process.

Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis:

- Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written.
- Dynamic analysis activity takes place during latter phases of product development: at the very least, the product or component should be able to run. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing at Oracle. Automatic tools employ fuzzing technique to test network-accessible product interfaces and protocols, while manual tools require making the modifications by hand.

Oracle will not provide customers sensitive security assurance artifacts (including but not limited to static code analysis reports). Oracle will not submit its product to third-party static code assessments. For more information, see MOS Article: General Instructions for Submitting Security Questionnaires to Oracle (Doc ID 2337651.1).

Security Fixing Policies

The Critical Patch Update (CPU) is the primary mechanism for the backport of security bug fixes for all Oracle on-premises products. Critical Patch Updates are available to customers with valid support contracts. Critical Patch Updates are released quarterly on the third Tuesday of January, April, July, and October. Oracle retains the ability to issue out of schedule patches or workaround instructions in case of particularly critical vulnerabilities and/or when active exploits are reported in the wild. This program is known as the Security Alert program. Vulnerabilities are remediated by Oracle in order of the risk they pose to users. This process is designed to patch the security defects with the greatest associated risk first in the Critical Patch Update, resulting in optimizing the security posture of all Oracle customers.

A standardized CPU schedule helps organizations plan their security maintenance windows. The CPU schedule is designed to avoid typical blackout dates during which customers cannot typically alter their production environments.

As much as possible, Oracle tries to make Critical Patch Updates cumulative; that is, each Critical Patch Update contains the security fixes from all previous Critical Patch Updates. This provides customers the ability to catch up quickly to the current security release level, since the application of the latest cumulative CPU resolves all previously addressed vulnerabilities.

Applicability of Critical Patch Updates and Security Alerts to Oracle Cloud Environments

The Oracle Cloud operations and security teams regularly evaluate Oracle's Critical Patch Updates and Security Alerts as well as relevant third-party security updates as they become available and apply the relevant patches in accordance with applicable change management processes.

Source Code Protection

Oracle maintains strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories.

Oracle Software Security Assurance policies and practices are designed to prevent the introduction of security vulnerabilities in Oracle-developed code. Additionally, Oracle maintains strong controls over the technical description of security vulnerabilities in Oracle code. Oracle's Security Vulnerability Information Protection Policy defines the classification and handling of information related to product security vulnerabilities and requires that information concerning security bugs be recorded in a tightly controlled database.

Oracle's policies prohibit the introduction of backdoors into its products. Backdoors are deliberately (and maliciously) introduced code intended to bypass the security controls of the application in which it is embedded. Backdoors do not include:

- Unintentional defects in software that could lead to a weakening of security controls (security bugs)
- Undocumented functionality designed to be generally inaccessible by customers but serves a valid business or technical purpose (diagnostics and troubleshooting utilities)

Oracle assesses third-party software and hardware to avoid the use of products:

- With known vulnerabilities
- Developed with poor security assurance
- That may potentially include backdoors or other malicious components

External Security Evaluations

Oracle submits certain products for external security evaluations. These evaluations involve rigorous testing by independently accredited organizations ("labs") with further oversight and certification completed by government bodies. Independent verification helps provide additional assurance to Oracle customers with regards to the security posture of the validated products. Organizaations in many industries have business and compliance requirements that imply the use of validated products. Such evaluations include Common Criteria and FIPS 140.

RESILIENCE MANAGEMENT

Oracle's risk management resiliency policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation and executive approvals for critical business operations.

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle's operations.

The RMRP approach is comprised of several subprograms: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.

Each of these subprograms is a uniquely diverse discipline. By consolidating emergency response, crisis management, business continuity and disaster recovery, they can become a robust collaborative and communicative system.

REVISION HISTORY

Version 3.3	04 Apr 2024	Updated introduction, information security incident response and Oracle Software Security Assurance sections
Version 3.2	12 Sep 2023	Clarified physical security and technical vulnerability management controls
Version 3.1	20 Jan 2023	Expanded Oracle Software Security Assurance (OSSA) section and updated the order of sections.
Verison 3.0	30 Sep 2022	Updates to all sections.
Version 2.1	20 May 2021	Clarified operational responsibilities for Incident Response.
Version 2.2	10 Sep 2021	Added wireless network management practices. Updated Operations Management, Incident Response, Technical Vulnerability Management and Access Control sections.
Version 2.3	22 Apr 2022	Clarified Global Information Security and Incident Response sections