Data Processing Agreement for Oracle European Union Sovereign Cloud ("Data Processing Agreement")

Version June 2, 2025

1. Scope and Applicability

This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the European Union Sovereign Cloud ("**EUSC**") Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement. In the event of any conflicting provisions between the terms of the Services Agreement (including any Services Descriptions and Service Specifications referenced therein) and the terms of this Data Processing Agreement, the terms of the Data Processing Agreement shall take precedence.

2. Responsibility for Processing of Personal Information and Description of Processing Activities

2.1 You are a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable European Data Protection Law.

2.2 Oracle will Process Personal Information during the term of the Services Agreement solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In particular and depending on the Services, Oracle may Process Personal Information for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.4 As part of the provision of the Services and depending on the Services, Oracle may Process Personal Information about Your Individuals, including Your end users, employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Personal Information about Your Individuals may include, but is not limited to, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; geolocation data; IP addresses and online behavior and interest data.

2.6 Unless otherwise specified in the Services Agreement, You may not provide Oracle with any data that imposes specific data security, data protection or regulatory obligations on Oracle in addition to or different from those specified in the Data Processing Agreement or Services Agreement (e.g. certain regulated health or payment card information). If available for the Services, You may purchase additional services from Oracle (e.g., Oracle Payment Card Industry Compliance Services) designed to address specific data security or data protection requirements applicable to sensitive or special data You seek to include in Your Content. You remain responsible for compliance with Your specific regulatory, legal or industry data security obligations which may apply to such data.

2.7 Additional or more specific descriptions of Processing activities may be included in the Services Agreement.

3. Your Instructions

3.1 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable European Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable European Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable European Data Protection Law relevant to Your use of the Services.

3.2 Oracle will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable European Data Protection Law. Oracle will immediately inform You if, in its opinion, Your instruction infringes Applicable European Data Protection Law. Oracle is not responsible for providing legal advice to You.

3.3 To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to

comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

4. Privacy Inquiries and Requests from Individuals

4.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by Oracle under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address the request. Additional information on how to access the Services to address privacy requests or inquiries from Individuals is available in the applicable Oracle Product or Service Feature Guidance documentation available on My Oracle Support (or other applicable primary support tool or support contact provided for the Services).

4.2 To the extent access to the Services is not available to You or otherwise not responsive to the request or inquiry, You can submit a "service request" via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to Oracle on how to assist You with such request.

4.3 If Oracle directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

5. Oracle Affiliates and Third Party Subprocessors

5.1 Subject to the restrictions set out in Section 6 below, You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

5.2 To the extent Oracle engages such Third Party Subprocessors and/or Oracle Affiliates, it requires that such entities are subject to the same level of data protection and security as Oracle under the terms of this Data Processing Agreement and Applicable European Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Information. Oracle remains responsible for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of the Data Processing Agreement and the Services Agreement.

5.3 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. The list of Oracle Affiliates for EUSC is available via https://www.oracle.com/corporate/oracle-affiliates/ (Section 3 – EU Sovereign Cloud) and the list of Third Party Subprocessors is available via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services). To receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, You can sign up per the instructions on My Oracle Support, Document ID 2288528.1.

5.4 Within thirty (30) calendar days of Oracle providing such notice to You under Section 5.3 above, You

may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services by submitting a "service request" via My Oracle Support (or other applicable primary support tool). You and Oracle will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable European Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 5.4 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

6. EU Processing and Cross-border Personal Information Transfer Restrictions

6.1 This Section 6 takes precedence over any conflicting provisions in Oracle's privacy policies and the Service Specifications. Pursuant to the technical, organizational and legal safeguards described in the applicable Service Descriptions and Hosting and Delivery Policies for EUSC, Oracle may store and Process Personal Information only within the selected EUSC data center region(s), unless otherwise instructed by You as described in Section 6.2.

6.2 Where instructed by You as described in the applicable Service Descriptions and Hosting and Delivery Policies for EUSC, You acknowledge that Personal Information may be Processed outside the selected EU data center region(s), such as when You enable a third party service or connect with an Oracle Cloud service that is hosted outside the EU data center region.

6.3 To the extent the instructions under Section 6.2 result in a Transfer of Personal Information subject to cross-border transfer restrictions under Applicable European Data Protection Law to countries outside Europe not covered by an adequacy decision. such transfers are subject to adequate data transfer safeguards, in particular (i) Oracle's Binding Corporate Rules for Processors or BCR-p (also referred to as the Oracle Processor Code) and (ii) the terms of Module 2 (Controller to Processor) or Module 3 (Processor to Processor) as applicable of the EU Standard Contractual Clauses 2021/914 of 4 June 2021. The Oracle Processor Code and Modules 2 and, as appropriate, Module 3 of the EU Standard Contractual Clauses will be read in conjunction with the Services Agreement and the Data Processing Agreement.

The most current version of the Oracle Processor Code is available on https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing, and is incorporated by reference into the Services Agreement and this Data Processing Agreement. Oracle has obtained EEA authorization for its Processor Code and will maintain such authorization for the duration of the Services Agreement. Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with the Oracle Processor Code, the terms of Module 3 (Processor to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021, this Data Processing Agreement and the Services Agreement.

6.4 Where applicable as set out in Section 6.2, the parties will review any supplemental measures, which may be required based on Applicable European Data Protection Law for the transfer of Personal Information to countries that do not offer an adequate level of protection. The parties will work together in good faith to find a mutually acceptable resolution to address such supplementary measures, including but not limited to reviewing technical documentation for the Services, and discussing additional available

technical safeguards and security services.

7. Security and Confidentiality

7.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services:

- **The Service Description for EUSC**, available at Oracle PaaS and IaaS Universal Credits Service Descriptions and/or, as applicable, **the Service Description for EUSC for Oracle Fusion Applications**, available at Oracle Fusion Service Descriptions;
- **Oracle's Corporate Security Practices**, available at https://www.oracle.com/corporate/security- practices/;
- **Oracle's Cloud Hosting & Delivery Policies**, available at Oracle Cloud Hosting and Delivery Policies;

7.2 All Oracle and Oracle Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

8. Audit Rights and Assistance with Data Protection Impact Assessments

8.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year, including inspections of the applicable Services data center facility that hosts Personal Information. In addition, to the extent required by Applicable European Data Protection Law, You or Your Regulator may perform more frequent audits.

8.2 If You engage a third party auditor, the third party must be mutually agreed to by You and Oracle (except if such third party is a Regulator). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to

Oracle or otherwise be bound by a statutory or legal confidentiality obligation.

8.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

8.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

8.5 Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

8.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

8.7 Without prejudice to the rights granted in Section 8.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

8.8 You may also request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations.

8.9 Oracle provides You with information and assistance reasonably necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and Oracle Product/Service privacy & security functionality guides for the Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Services or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to You.

9. Incident Management and Breach Notification

9.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Your Content (as such term is defined in the Services Agreement) transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if an Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

9.2 Oracle will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information and approximate number of Individuals that were the subject of the Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

10. Return and Deletion of Personal Information

10.1 Upon termination of the Services, Oracle will promptly return, including by providing available data retrieval functionality, and subsequently delete any remaining copies of Personal Information on Oracle systems or Services environments, except as otherwise stated in the Services Agreement.

10.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by Oracle as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

11. Legal Requirements

11.1 Subject to the technical, organizational and legal safeguards described in the Hosting and Delivery Policies for EUSC, Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

11.2 Oracle will promptly inform You of requests to provide access to Personal Information and use reasonable efforts to redirect the authority that made the request to You, unless otherwise required by law.

11.3 To the extent Oracle is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on Oracle, including whether the request is consistent with Applicable European Data Protection Law. Any request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law. Oracle will provide the minimum amount of Personal Information strictly necessary when responding to a request.

12. Data Protection Officer

12.1 Oracle has appointed a Chief Privacy Officer and a local Data Protection Officer in certain countries. Further details on how to contact Oracle's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available at https://www.oracle.com/legal/privacy/index.html.

12.2 If You have appointed a Data Protection Officer, You may request Oracle to include the contact details of Your Data Protection Officer in the relevant Services order.

13. Definitions

"**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act on Data Protection, as amended.

"**Europe"** means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Liechtenstein and Norway; and (ii) Switzerland.

"**Individual"** shall have the same meaning as the term "data subject" or the equivalent term under Applicable European Data Protection Law.

"**Information Breach"** means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Your Content transmitted, stored or otherwise Processed on Oracle systems or the Services environment that results in the actual or potential loss of confidentiality, integrity or availability of Your Content.

"**Process/Processing**", "**Controller**", "**Processor**" and "**Binding Corporate Rules**" (or the equivalent terms) have the meaning set forth under Applicable European Data Protection Law.

"**Oracle Affiliate(s)**" means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in this Data Processing Agreement.

"**Oracle**" means the Oracle Affiliate that has executed the Services Agreement.

"**Personal Information**" shall have the same meaning as the term "personal dataμ or the equivalent term under Applicable European Data Protection Law.

"**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable European Data Protection Law.

"**Services**" or the equivalent terms "Service Offerings" or "services" means the EUSC Services specified in the Services Agreement.

"**Services Agreement**" means (i) the applicable order for the Services you have purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications, including the applicable Service Description and Hosting and Delivery Policies for the EUSC.

"**Third Party Subprocessor**" means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in this Data Processing Agreement.

"**Transfer**" means the possible or actual access by, transfer or delivery to, or disclosure of Personal Information to a person, entity or system located in a country or jurisdiction outside the EU/EEA, including any subsequent processing operations performed in such country or jurisdiction;

"**You**" means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.