Crown Commercial Service

RM6292 Cloud Compute
Annex 5 to Framework Schedule 4

Template Order Form, Lot 3 – Professional Services

1. This Order Form is issued in accordance with the provisions of the Cloud Compute 2 Framework Agreement RM6262 dated 17-NOV-2023 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after conducting a further competition or a direct award under the Framework Agreement.
2. The Contract, referred to throughout this Order Form, means the contract (entered into pursuant to the terms of the Framework Agreement) between the Supplier and the Buyer (as defined below) consisting of this Order Form and the Professional Services Call-Off Terms set out in Annex 1 (and which are substantially the terms set out in Annex 5 to Schedule 4 to the Framework Agreement) and copies of which are available from the Crown Commercial Service website *https://www.crowncommercial.gov.uk*.
3. The Supplier shall provide the Services specified and/or referred to in this Order Form (including any attachments to this Order Form) to the Buyer and the Buyer Users on and subject to the terms of the Contract for the duration of the Contract Period. The Contract shall take effect on the Commencement Date (as defined below) and shall expire at the end of the Contract Period.
4. In this Order Form, unless the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Professional Services Call-Off Terms.
5. This Order Form shall comprise:
   (a) This document headed "Order Form";
   (b) Attachment 1 – Charges and Payment Profile;
   (c) Attachment 2 – Schedule of Standards;
   (d) Attachment 3 – Schedule of Processing, Personal Data and Data Subjects;
   (e) Attachment 4 – Alternative Clauses;
   (f) Attachment 5 – List of Transparency Reports;
   (g) Attachment 6 – Service Descriptions and Product Terms;
   (h) Attachment 7 – Deliverables;
   (i) Attachment 8 – Data Processing Agreement; and
   (j) Annex 1 – Professional Services Call-Off Terms.
6. The Order of Precedence shall be as set out in Clause 2.2 of the Professional Services Call-Off Terms being:
   (a) subject always to Clauses 2.4 and 4.2.2 of the Call-Off Terms, the Special Terms (if any);
   (b) this Order Form (except Special Terms (as defined in the Professional Services Call-Off Terms));
   (c) the Professional Services Call-Off Terms;
   (d) the applicable provisions of the Framework Agreement, except (and subject always to Clause 2.4 and 4.2.2 of the Professional Services Call-Off Terms) Schedule 13 (Tender) of the Framework Agreement; and
   (e) Schedule 13 (Tender) of the Framework Agreement.
7. Where Schedule 13 (Tender) of the Framework Agreement contains provisions which are more favourable to the Buyer in relation to this Contract such provisions of the Tender (as applicable) shall prevail. The Buyer shall in its absolute and sole discretion determine whether any provision in the Tender and/or this Contract is more favourable to it in this context.

8. Special Terms shall only apply to this Contract if they:

   (a) are set out in full in the section of this Order Form entitled “Special Terms”; and

   (b) augment and supplement this Contract and in particular do not amend the Call-Off Terms to any material extent,

   and provided always that any attempt to incorporate by reference any Supplier Terms as Special Terms in this Contract shall be ineffective.

9. Alternative Clauses specified in this Order Form will take precedence over their corresponding clauses in this Contract.

Crown Commercial Service

Section A - General information:

Contract Details	
Contract Reference:	ecm_12598
Contract Title:	Professional services for DWP Personal Independence Payments (PIP), Child Maintenance Services (CMS) and Customer Information System (CIS)
Contract Description:	Professional services to migrate the DWP PIP, CMS and CIS from On Premise Hosting (OPH) to Oracle Cloud Infrastructure (OCI)
Commencement Date:	07-FEB-2025

Buyer details

Buyer organisation name:

Department for Work and Pensions (DWP), referenced in this Order Form as either "You", "Your", "Buyer" or "DWP" (all variations meaning the same)

Billing address:

Brunel Way, Blackpool Fylde Industrial Estate, Blackpool & Fylde Industrial Estate, GB, FY4 5DR

Buyer Authorised Representative name:

REDACTED FOI 40

Buyer Authorised Representative contact details:

Address:

REDACTED FOI 40

Buyer's Data Protection Officer name:

REDACTED FOI 40

Buyer's Data Protection Officer contact details:

Crown Commercial Service

REDACTED FOI 40

Supplier details

Supplier name:

Oracle Corporation UK Limited, referenced in this Order Form as either the "Supplier" or "Oracle" (all variations meaning the same)

Supplier address:

Oracle Parkway, Thames Valley Park, Reading, Berkshire RG6 1RA

Supplier authorised representative name:

REDACTED FOI 40

Supplier authorised representative contact details:

REDACTED FOI 40

Order reference number:

ecm_12598

Key Sub-Contractors and Sub-processors:	There are no sub-contractors involved in the delivery of the Services. The Sub-processors are set out in the Supplier's Register of Sub-processors which is available at: https://buyers.procserveonline.com. Subject always to Clause 15.12 of the Call-Off Terms, the Supplier is obliged to maintain the Register of Sub-processors in accordance with Clause 15.1 of the Framework Agreement. Where the Supplier intends to appoint or replace a Sub-processor not identified as a Sub-processor in the Supplier's Register of Sub-processors at the Commencement Date, any such changes shall be subject always to Clause 15.12 of the Call-Off Terms.

Crown Commercial Service

Section B - The Services Requirement:

Commencement Date:
As per Section A above.

Initial Term:

Twelve (12) months from the Commencement Date.

Extension Period:

This Contract can be extended for a maximum of two (2) periods of up to twelve (12) months each (each an 'Extension Period') beyond the Initial Term or the extended Initial Term (as applicable), up to a maximum term of thirty-six (36) months from the Commencement Date.

Special Security or compliance requirements:

(a) The Buyer's Security Level Assessment (SLA) has determined a level 4 assessment as the minimum security requirement for the Buyer for these services. The Supplier agrees to reasonably work with the Buyer to carry out a further assessment of the Buyer's minimum security requirements against the Supplier's own security policies within three (3) months of the Commencement Date and to report every twelve (12) months, as part of operational service management reviews, any gaps between the Buyer minimum security requirements and the Supplier's own policies, but the Buyer and Supplier each acknowledge and agree that the Supplier's own security policies and procedures continue to apply throughout the duration of this Order Form (including any Extension Periods).
(b) Subject to paragraph (a) above, within three (3) months of the Commencement Date of this Order Form, the Supplier will provide the Buyer with any relevant physical security polices/standards/procedures that evidence that the Supplier has adequate physical security controls in place, that specifically cover the following elements, to the extent applicable to the Services:

a) carry out physical security audits/reviews periodically;
b) clear-screen policy for papers, removable media and information processing facilities;
c) physical security controls in place to protect secure areas including visitor access;
d) controls in place to protect equipment and facilities against natural disasters and other incidents or interruptions, malicious or otherwise;
e) monitor physical access and review access logs to the facilities to detect and respond to physical security incidents;
f) controls in place to protect cables carrying data against interception, interference or damage.

Special Terms:

Insert any specific contractual provisions below which are hereby incorporated into the Contract. Should the Buyer be eligible for a Government Discount according to the Supplier's eligibility criteria and wish to activate the Government Discount, it should indicate this here and the following variations would then be treated as amending the Order Form and Professional Services Call-Off Terms.

1. Government Discount(s)

N/A

2. Social Value
The Buyer will be monitoring the Supplier social value contributions in relation to the two themes stated below.

The Parties will agree the performance levels, reporting metrics and reporting format for these metrics within three (3) months from the Commencement Date and the Supplier will report on these monthly thereafter:

- Theme 2: Tackling economic inequality;
- Theme 4: Reduce the disability employment Gap.

3. Professional Services Delivery Policies

The Professional Services Delivery Policies are set out in Appendix 2 to the Product Terms attached as Exhibit B (Oracle Product Terms) to this Order Form. The Policies are subject to change from time-to-time, but such changes will not materially reduce the level of performance, security, or availability of the Services under this Order Form for the duration of this Order Form. Further, the Policies contain words, phrases or specific web addresses that allow the Buyer to click through to another section of the same documentor to a URL which contains a policy, terms and conditions or any other document ("**Additional Hyperlinks**"). To the extent only the then- current and appropriately localised Additional Hyperlinks that apply to the Services provided under this Order Form, such Additional Hyperlinks apply, and are incorporated by reference, to this Order Form. Where the Supplier has used Additional Hyperlinks in the Policies to supplement the Policies, the Supplier shall, for the duration of this Order Form, not materially reduce the level of performance, security, or availability of the Services under this Order Form.

In addition, the Supplier updates to Policies will not: (a) increase the fees specified in the Order Form for the quantity of Services purchased in respect of each Statement of Work ("SOW") to be delivered in accordance with Attachment 7 (Deliverables) (each a "Delivery SOW") under this Order Form for the duration of this Order Form or (b) have a negative and detrimental effect on the Buyer's contractual rights and/or obligations.

Services:

This Order Form is for the Services set out or referred to below. It is acknowledged by the Parties that the volume of the Services consumed by the Buyer and/or Buyer Users may vary during the Contract as provided for below.

Please provide details of all Services required to be in scope of the Contract with appropriate references, where available, from the Catalogue as defined in Schedule 1 (Definitions) of the Framework Agreement.

Professional Services Terms required:	For the Services to be provided by the Supplier: see Attachment 6 (Service Descriptions and Product Terms) for those Services which are potentially in scope; and each Delivery SOW of Attachment 7 (Deliverables) for the description of Services and Deliverables to be provided under this Order Form.
Service Request process (dynamic nature of Services):	Not Applicable
Geographical limitations on the location(s) from which the Services will be provided:	The Services are to be provided from the United Kingdom, offshoring and any other option is out of scope for this Order Form and is not permitted. **Restricted Country**: ☑ **Location:** United Kingdom
Standards:	In addition to complying with Clause 3.2 of the Professional Services Call-Off Terms, including those Standards set out in Attachment 2 (Schedule of Standards) to this Order Form and the Framework Agreement, the additional standards the Supplier is required to comply with under the Contract are: Not applicable for any other additional standards.

On-boarding:	Not Applicable
Off-boarding:	The Supplier shall as part of off-boarding: (i) handover all Deliverables in the format specified in each Delivery SOW of Attachment 7 that the Buyer has already paid for at the date of off-boarding and (ii) unless agreed otherwise in writing by the Buyer, promptly return Buyer equipment and any access passes provided to the Supplier by the Buyer.
Force Majeure:	In respect of a Force Majeure event, the reference to twenty (20) Working Days set out in Clause 29.4 of the Professional Services Call-Off Terms shall be shortened to: Not Applicable
Audit:	In addition to the audit rights set out in Clause 13 of the Professional Services Call-Off Terms, the following additional audit rights shall apply to the Contract: Section 15 of the Product Terms The Supplier shall not require any Buyer to disapply its audit rights under Clause 13 of the Professional Services Call-Off Terms and this Order Form (if any) as a condition to providing the Services.

Charges and payment:

The Charges applicable to the Contract and payment details are set out in the table immediately below.

Charges **(including applicable discount(s)/ preferential pricing and exclusive of VAT):**	The Charges payable by the Buyer to the Supplier in respect of each Delivery SOW are as set out in the Milestone Payment Table of Attachment 1 (Charges and Payment Profile) to this Order Form.
Charges breakdown:	The breakdown of the Charges in respect of each Delivery SOW is as set out in Attachment 1 (Charges and Payment Profile) to this Order Form.
Currency:	All prices under this Contract shall be quoted exclusively in: Pounds Sterling unless otherwise agreed in writing by the Buyer Authorised Representative. All Charges shall be paid and/or payable exclusively in Pounds Sterling.
Currency and currency conversion mechanism:	In accordance with Clause 7.5 of the Professional Services Call-Off Terms, where the Charges under this Contract are stated (priced) in a currency other than Pounds Sterling then any invoiced amounts due under this Contract shall be calculated in accordance with the following currency conversion mechanism: Not Applicable
Payment method:	The payment method for this Contract is via a Purchase Order. The purchase order must be in a non-editable format (e.g. PDF) and include the following information: • Order Reference Number • Total Price (excluding applicable tax) • Local Tax, if applicable

	In issuing a purchase order, the Buyer agrees that no terms included in any such purchase order shall apply to the Services ordered under this Order Form.
Payment profile:	The payment profile is set out in Attachment 1 (Charges and Payment Profile) in respect of each Delivery SOW.
Invoice details and frequency:	The Supplier will issue an invoice (including any Electronic Invoices) in accordance with the Payment profile set out above. Pursuant to Clause 7.4 of the Professional Services Call-Off Terms, the Buyer will pay the Charges to the Supplier within thirty (30) days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent by the Supplier to the Buyer at: REDACTED FOI 24
Invoice information required:	The Billing Entity on all invoices has to be in the UK, with a UK address and all invoices must include: • a valid Purchase Order (PO) number With respect to the PO Number (if applicable), the Buyer must provide its PO number no later than seven (7) days after the execution of this Order Form. If no PO number is provided by the Buyer within the time period specified in this paragraph or at all, the Buyer agrees and acknowledges that the Supplier can invoice the Buyer without a PO number in the applicable invoice(s), and such invoice is still due and payable in accordance with terms of this Call-Off Contract.
Contract anticipated potential value:	The initial Delivery Statement of Work (SOW 1) as set out in Attachment 7 has a value of **£1,200,000.00** (exclusive of VAT) (as detailed in Attachment 1 (Charges and Payment Profile). The Buyer anticipates that the total Contract value is up to a maximum of **£4,250,000.00** (exclusive of VAT) but any additional Delivery SOWs to be incorporated into Attachment 7 (Deliverables) must be agreed by both the Buyer (subject to the Buyer's governance approvals) and Supplier in writing as a variation to this Contract using the variation procedure set out in clause 28 of the Professional Services Call-Off Terms.

Additional Buyer terms:

Liability:	For the purpose of Clause 9.1 of the Professional Services Call-Off Terms the reference to "five million pounds (£5,000,000)" is replaced with the following higher limit: Not Applicable. For the purpose of Clause 9.4 of the Professional Services Call-Off Terms the reference to "ten million pounds (£10,000,000)" is replaced with the following higher limit: Not Applicable.
Buyer specific amendments to/	Within the scope of this Order Form, the following applies:

refinements of the Contract terms:	**1. Transfer of Undertakings (Protection of Employment) TUPE** Appendix 5 (TUPE) to the Oracle Product Terms set out in Exhibit B (Oracle Product Terms) applies to this Contract. **2. Acceptance of Deliverables** (a) Upon the earlier of the occurrence of: (i) completion of the applicable deliverable described in Attachment 7 (Deliverables) or (ii) completion of a milestone set forth in the Milestone Payment Table of Attachment 1(Charges and Payment Profile) the Supplier shall provide a copy of the deliverables to the Buyer in the deliverable format set out in Attachment 7 (Deliverables). At such time, if the Buyer requests, the Supplier will demonstrate to the Buyer that the deliverable conforms to the description specified for such deliverable in the Milestone Delivery Table of the Delivery SOW or acceptance criteria set forth in Milestone Delivery Table of the Delivery SOW or such other criteria that is mutually agreed between the parties during the project and documented accordingly ("**Acceptance Criteria**"). Where the parties seek to agree different acceptance criteria, in the event the parties are unable to agree such acceptance criteria for a deliverable,then either party may invoke the Dispute Resolution Procedure set out in paragraph (c) below of this section 2.The Buyer will be responsible for any additional review of such deliverable in accordance with any mutually agreed scripts/tasks as may be included in the Supplier's project management plan. If the deliverable does not conform with the description for such deliverable specified in the Milestone Delivery Table, the Delivery SOW and/or any such Acceptance Criteria, the Buyer shall have ten (10) business days after the Supplier's submission of the deliverable ("**Acceptance Period**") to give the Supplier confirmed acceptance in writing or written notice which shall clearly state in detail any material non-conformance against Acceptance Criteria of the specified deliverable. Supplier shall use reasonable efforts to promptly cure any such deficiencies and resubmit the affected deliverable in accordance with the paragraph (b) below; (b) After completing such cure, the Supplier shall resubmit the deliverable for the Buyer's review without unreasonable delay. Upon accepting any deliverable submitted by the Supplier, the Buyer shall provide the Supplier with written acceptance of such deliverable within the Acceptance Period. In the event that confirmation of either acceptance or notification of failures is not received in writing by five (5) business days from the commencement of the Acceptance Period i.e. from day 1 to day 5, then the Supplier will use reasonable endeavors to remind the Buyer single point of contact to notify the Supplier in writing either the Buyer accepts the deliverable in question or details the deficiencies which need to be cured in accordance with this section. If the Buyer fails to provide written notice of any deficiencies or written acceptance within a further five (5) business days from the date of reminder by the Supplier, then it is acknowledged and agreed by the Buyer that there is no deficiency in the deliverables and such deliverables have been accepted by the Buyer; and (c) In the event of any dispute or disagreement between the parties arising out of or relating to this section 2 (Acceptance of Deliverables) (the "dispute"), the parties will endeavour to resolve the dispute in accordance with this paragraph (c). Either party may invoke this paragraph (c) by providing the other party written notice of its decision to do so, including a description of the issues subject to the dispute. Each party will appoint a Vice President (or equivalent level) ("**representative**") to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief, may be initiated by a party until either parties' representative concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. The parties shall refrain from exercising any termination

	right and shall continue to perform their respective obligations under this Order Form while the parties endeavour to resolve the dispute under this paragraph (c), provided that, any party alleged to be in breach promptly makes good faith efforts to cure such breach and pursues the cure in good faith. **3. Fees and Expenses** The Buyer agrees to pay the Supplier the applicable fees and any applicable taxes in respect of each Delivery SOW as set out in the Milestone Payment Table of Attachment 1 (Charges and Payment Profile) to this Order Form. There are no expenses other than those set out in the Milestone Payment Table of Attachment 1 (Charges and Payment Profile) (if applicable) in respect of each Delivery SOW. Upon completion of a milestone, the corresponding milestone fee for such milestone specified in the Milestone Payment Table of Attachment 1 (Charges and Payment Profile) in respect of each Delivery SOW becomes due and payable and the Supplier shall thereafter invoice, and the Buyer shall pay, such milestone fee; this payment obligation shall become non-cancellable and the sums paid non-refundable on such milestone completion date.
Personal Data and Data Subjects:	See Attachment 3 (Schedule of Processing, Personal Data and Data Subjects) to this Order Form.
Sites:	The Buyer does not prescribe the location the services will be delivered however there is likely to be a requirement that the Supplier will attend key Buyer sites at no additional expense charges. REDACTED FOI 24. Unless otherwise specified in the relevant Delivery SOW, the base location for the Supplier staff will be remote.
Buyer Property:	See section titled "Off-boarding" above in this Order Form.
Deliverables:	The Supplier shall provide the following Deliverables to the Buyer as part of the Services: As set out in Attachment 7 (Deliverables) to this Order Form.

Alternative Clauses:

The following Alternative Clauses will apply:	Scots Law - Not Applicable Northern Ireland Law - Not Applicable HMRC Terms - Not Applicable Where selected above (if any) the Alternative Clauses set out in Attachment 4 (Alternative Clauses) of this Order Form shall apply as indicated to the Contract.

Crown Commercial Service

Section C - Commercially Sensitive information:

Commercially Sensitive information:

Any information that the Supplier considers sensitive for the duration of the Order Form is stated below:

No.	Date	Item(s)	Duration of Confidentiality
1	Any	Pricing (except to the extent that this has to be disclosed in the OJEU contract award notice or to comply with the UK governments' transparency agendas) especially the way in which the Supplier has arrived at the aggregate contract price, any information revealing the different constituent elements of the aggregate contract price, day rates. Information relating to the Supplier's costs. Information as to the proposed level of discounts offered.	Contract term + 5 years
2	Any	The Supplier's (or any member of the Supplier's group's) intellectual property. All information that is not in the public domain relating to the Supplier's (or any member of the Supplier's group's) intellectual property rights, solution design and methodologies including all templates, method statements, workshop agendas, detailed implementation plans and resourcing profiles. Any product or service roadmaps relating to potential future developments.	Indefinitely
3	Any	Information relating to product or service performance or vulnerabilities including security vulnerabilities. Any test results.	Indefinitely
4	Any	Information not in the public domain relating to the Supplier group's business or investment/ divestment plans, financial standing - Indefinitely	Indefinitely
5	Any	Information not in the public domain relating to any litigation or disputes that the Supplier group is a party to.	Indefinitely
6	Any	Details of the Supplier's suppliers, partners and sub-contractors and technology used to provide the Services (including all information relating to Key Subcontractors)	Indefinitely
7	Any	Personal data relating to the Supplier's members of staff and anybody else working on the contract. Terms and conditions of employees.	Indefinitely
8	Any	Details of the Supplier's insurance arrangements.	Indefinitely

Crown Commercial Service

Section D - Contract award:

The Contract is awarded in accordance with the provisions of the Framework Agreement.

SIGNATURES

Name:	REDACTED FOI 40
Job role/title:	REDACTED FOI 40
Signature:	REDACTED FOI 40
Date:	10 February 2025

Name:	REDACTED FOI 40
Job role/title:	REDACTED FOI 40
Signature:	REDACTED FOI 40
Date:	11 February 2025

Crown Commercial Service

Attachment 1 – Charges and Payment Profile

SOW Control Table

SOW#	Descriptor
SOW#1	**PIP and CMS Design and Initial Build/Unit Test Phase**

1. SOW#1 Charges

(a) The charges in respect of this Delivery SOW#1 are as set out in the table below and shall be payable in accordance with the terms of sub-section 2. "Acceptance of Deliverables" and sub-section 3. "Fees and Expenses" of the section titled "Buyer specific amendments to/ refinements of the Contract terms" of this Order Form.
(b) Oracle will not invoice DWP for personal expenses i.e., travel, accommodation, etc. for this project.

Milestone Payment Table

Milestone #	Supplier Milestone & Descriptor	Milestone reference to the DWP 8 Phase Methodology	Milestone Payment (Excluding VAT)	Milestone Target Due Date
	REDACTED IN FULL FOI 24 & 43			
		Total	**£1,200,000.00**	

Crown Commercial Service

Attachment 2 – Schedule of Standards

1. The Supplier shall comply with the following Standards:

   1.1. the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications;

   1.2. guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets;

   1.3. the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection;

   1.4. government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice;

   1.5. the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles;

   1.6. ISO 27001 Information Security Management standard, and provide the Buyer with the relevant certification, if requested by the Buyer;

   1.7. ISO 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, and provide the Buyer with the relevant certification, if requested by the Buyer;

   1.8. ISO 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, and provide the Buyer with the relevant certification, if requested by the Buyer;

   1.9. BS EN ISO 9001 "Quality Management System" standard or equivalent;

   1.10. BS EN ISO 14001 Environmental Management System standard or equivalent; and

   1.11. any additional Standards set out or referred to in this Order Form.

2. If a Buyer has requested in this Order Form that the Supplier has a Cyber Essentials Plus certificate, the Supplier must provide the Buyer with a valid Cyber Essentials Plus certificate required for the Services before the Commencement Date. (https://www.ncsc.gov.uk/cyberessentials/overview).

Notwithstanding the above, please be aware that not all services provided by the Supplier comply with every one of the Standards (as defined). When placing any orders via the Supplier Portal it is the Buyer's responsibility to check with the Supplier the applicable compliance status before taking a decision to placing/entering into any order.

Crown Commercial Service

Attachment 3 – Schedule of Processing, Personal Data and Data Subjects

Attachment 3 is not applicable as the Buyer will not disclose any Personal Data to the Supplier.

This Attachment 3 shall be completed by the Buyer, who may take account of the view of the Supplier, however the final decision as to the content of this Attachment 3 shall be with the Buyer at its absolute discretion.

1. The contact details of the Buyer's Data Protection Officer are: [*Insert Contact details*].
2. The contact details of the Supplier's Data Protection Officer are: [*Insert Contact details*].
3. The Supplier shall comply with any further written instructions with respect to processing by the Buyer.
4. Any such further instructions shall be incorporated into this Attachment 3.

Description	Details
Identity of the Controller and Processor:	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor in accordance with Clause 15 (Protection of Personal Data) of the Professional Services Call-Off Terms.
Subject matter of the processing:	*[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.* *Example: The processing is needed in order to ensure that the Supplier can effectively deliver the contract to provide a service to members of the public.]*
Duration of the processing:	*[Clearly set out* the duration of the *processing including dates]*
Nature and purposes of the processing:	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* • *The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]*
Type of Personal Data being Processed:	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]*
Categories of Data Subject:	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]*
Plan for return and destruction of the data once the processing is complete: **(UNLESS requirement under union or member state law to preserve that type of data)**	*[Describe how long the data will be retained for, how it be returned or destroyed]*

Crown Commercial Service

Attachment 4 – Alternative Clauses

Attachment 4 is not applicable to this Contract

Where the Buyer in Section B of this Order Form has requested Alternative Clause(s) to apply to the Contract, the requested Alternative Clause(s) shall apply to the Contract as follows:

A. SCOTS LAW

Governing Law, Jurisdiction and Dispute Resolution (Clauses 33.1 and 33.5 of the Professional Services Call-Off Terms):

(a) References to "*England and Wales*" in the original Clauses 33.1 and 33.5 of the Professional Services Call-Off Terms (Governing Law, Jurisdiction and Dispute Resolution) shall be replaced with "*Scotland*".

(b) Where legislation is expressly mentioned in the Contract, the adoption of sub-paragraph (a) immediately above shall have the effect of substituting the equivalent Scots legislation.

B. NORTHERN IRELAND LAW

Governing Law, Jurisdiction and Dispute Resolution (Clauses 33.1 and 33.5 of the Professional Services Call-Off Terms):

(a) References to "England and Wales" in the original Clauses 33.1 and 33.5 of the Professional Services Call-Off Terms (Governing Law, Jurisdiction and Dispute Resolution) shall be replaced with "Northern Ireland".

(b) Where legislation is expressly mentioned in the Contract the adoption of sub-paragraph (a) immediately above shall have the effect of substituting the equivalent Northern Ireland legislation.

Insolvency Event

In Schedule 1 (Definitions) to the Professional Services Call-Off Terms, reference to "*section 123 of the Insolvency Act 1986*" in limb f) of the definition of Insolvency Event shall be replaced with "*Article 103 of the Insolvency (NI) Order 1989*".

C. HMRC Terms

1. Definitions

1.1. In these HMRC Terms, the following words have the following meanings and they shall supplement Schedule 1 (Definitions) to the Professional Services Call-Off Terms as follows:

Connected Company(ies)	means in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;
Government Data	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Buyer's and/or any Buyer User's Confidential Information, and which: a) are supplied to the Supplier by or on behalf of the Buyer and/or any Buyer User; or b) the Supplier is required to generate, process, store or transmit pursuant to the Contract. For the avoidance of any doubt Government Data shall include any Buyer Content;

Prohibited Transaction	means: a) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description otherwise payable by the Supplier or a Connected Company on or in connection with the Charges; or b) which would be payable by any Key Sub-contractor and its Connected Companies on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Sub-contract with that Key Sub-contractor, other than transactions made between the Supplier and its Connected Companies or a Key Sub-contractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business;
Tax Compliance Failure	means where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Exhibit 1 (Excerpt from HMRC's "Test for Tax Non-Compliance") to this Attachment 6 (as amended and updated from time to time), where: (a) the "Economic Operator" means the Supplier or any agent, supplier or Sub-contractor of the Supplier requested to be replaced pursuant to paragraph 4.2 (Promoting Tax Compliance) of Part C (HMRC Terms) as set out in Attachment 4 (Alternative Clauses) to the Order Form; and (b) any "Essential Subcontractor" means any Key Sub-contractor;

2. Application of these clauses

2.1. Where the Buyer is Her Majesty's Revenue and Customs (HMRC), as identified in Section B of this Order Form, and HMRC has requested these HMRC Terms to apply to the Contract, the requested Alternative Clause(s) shall apply to the Contract as follows.

3. Warranties

3.1. The Supplier represents and warrants that:

3.1.1. in the three years prior to the Effective Date, it has complied with all applicable Law related to Tax in the United Kingdom and in the jurisdiction in which it is established;

3.1.2. it has notified the Buyer in writing of any Tax Compliance Failure it is involved in; and

3.1.3. no proceedings or other steps have been taken (nor, to the best of the Supplier's knowledge, are threatened) for:

3.1.3.1. the winding up of the Supplier;

3.1.3.2. the Supplier's dissolution;

3.1.3.3. the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue,

and the Supplier has notified the Buyer of any profit warnings it has issued in the three years prior to the Commencement Date.

3.2. If the Supplier becomes aware that any of the representations or warranties under paragraph 3.1 of this Attachment 4, have been breached, are untrue or misleading, it shall immediately notify the Buyer in sufficient detail to enable the Buyer to make an accurate assessment of the situation.

3.3. In the event that the warranty given by the Supplier in paragraph 3.1 of this Attachment 4 is materially untrue, this shall be deemed to be a material Default which in the opinion of the Buyer is not capable

of remedy and in accordance with Clause 16.2.1 of the Professional Services Call-Off Terms the Buyer may at any time terminate this Contract with immediate effect by giving notice to the Buyer.

4. Promoting Tax Compliance

4.1. The Supplier shall comply with all Law relating to tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.2. The Supplier shall provide to the Buyer the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the corporation tax or self-assessment reference of any agent, supplier or Sub-contractor prior to that person supplying any Services under the Contract. Upon a request by the Buyer, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Sub-contractor engaged in supplying Services under the Contract.

4.3. If, at any point during the Contract Period, there is a Tax Compliance Failure, the Supplier shall:

4.3.1. notify the Buyer in writing within five (5) Working Days of its occurrence; and

4.3.2. promptly provide to the Buyer:

4.3.2.1. details of the steps which the Supplier is taking to resolve the Tax Compliance Failure and to prevent it from recurring, together with any mitigating factors that it considers relevant; and

4.3.2.2. such other information in relation to the Tax Compliance Failure as the Buyer may reasonably require.

4.4. The Supplier shall indemnify the Buyer against any liability for Tax (including any interest, penalties or costs incurred) of the Buyer in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under the Contract.

4.5. Any amounts due under paragraph 4.4 of this Attachment 4 shall be paid not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Buyer. Any amounts due under paragraph 4.4 of this Attachment 4 shall not be subject to Clause 9.1 of the Professional Services Call-Off Terms and the Supplier's liability under paragraph 4.4 of this Attachment 4 is unlimited.

4.6. Upon the Buyer's request, the Supplier shall promptly provide information which demonstrates how the Supplier complies with its Tax obligations.

4.7. If the Supplier:

4.7.1. fails to comply with paragraphs 4.1, 4.3.1 and/or 4.6 of this Attachment 4 this may be a material Default of the Contract;

4.7.2. fails to comply with a reasonable request by the Buyer that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by paragraph 4.2 of this Attachment 4 on the grounds that the agent, supplier or Sub-contractor is involved in a Tax Compliance Failure this shall be a material Default of the Contract; and/or

4.7.3. fails to provide acceptable details of the steps being taken and mitigating factors pursuant to paragraph 4.3.2 of this Attachment 4 this shall be a material Default of the Contract;

and any such material Default shall be deemed to be an event to which Clause 16.2.1 of the Professional Services Call-Off Terms applies and the Buyer's payment obligations under the Contract shall cease immediately as if the Contract had been terminated under Clause 16.2 of the Professional Services Call-Off Terms.

4.8. In addition to those circumstances listed in Clause 20.7 of the Professional Services Call-Off Terms, the Buyer may internally share any information, including Confidential Information, which it receives under paragraphs 4.2 and 4.3 of this Attachment 4 and 4.6 of this Attachment 4.

5. Use of Off-shore Tax Structures

5.1. The Supplier shall not, and shall ensure that its Connected Companies, Key Sub-contractors (and their respective Connected Companies) shall not, have or put in place any Prohibited Transactions, unless the Buyer otherwise agrees to that Prohibited Transaction.

5.2. The Supplier shall notify the Buyer in writing (with reasonable supporting detail) of any proposal for the Supplier, its Connected Companies, or a Key Sub-contractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall include reasonable supporting detail and make the notification within a reasonable time before the Prohibited Transaction is due to be put in place.

5.3. If a Prohibited Transaction is entered into in breach of paragraph 5.1 of this Attachment 4, or circumstances arise which may result in such a breach, the Supplier and/or the Key Sub-contractor (as applicable) shall discuss the situation with the Buyer. The Parties shall agree (at no cost to the Buyer) any necessary changes to any such arrangements by the undertakings concerned (and the Supplier shall ensure that the Key Sub-contractor shall agree, where applicable). The matter will be resolved using Clause 33 (Governing Law, Jurisdiction and Dispute Resolution) of the Professional Services Call-Off Terms if necessary.

5.4. Failure by the Supplier (or a Key Sub-contractor) to comply with the obligations set out in paragraphs 5.2 and 5.3 of this Attachment 4 shall be deemed to be an event to which Clause 16.2.1 of the Professional Services Call-Off Terms applies and the Buyer's payment obligations under the Contract shall cease immediately as if the Contract had been terminated under Clause 16.2 of the Professional Services Call-Off Terms.

6. Data Protection and off-shoring

6.1. For the purposes of Clause 15.4.4 of the Professional Services Call-Off Terms a reference to a Restricted Country shall mean any country other than the United Kingdom.

7. Commissioners for Revenue and Customs Act 2005 and related Legislation

7.1. The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Government Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ("**CRCA**") to maintain the confidentiality of Government Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to a prosecution under Section 19 of CRCA.

7.2. The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Government Data comply with the obligations set out in the Official Secrets Acts 1911 to 1989 and the obligations set out in Section 182 of the Finance Act 1989. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to prosecution under those Acts.

7.3. The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Government Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

7.4. The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Government Data in writing of the obligations upon Supplier Personnel set out in paragraphs 7.1, 7.2 and 7.3. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

7.5. The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Government Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Exhibit 2 (Confidentiality Declaration) to this Attachment 4. The Supplier shall provide a copy of each such signed declaration to the Buyer upon demand.

7.6. In the event that the Supplier or the Supplier Personnel fail to comply with this paragraph 6, the Buyer reserves the right to terminate the Contract as if that failure to comply were an event to which Clause 16.2.1 of the Professional Services Call-Off Terms applies.

Crown Commercial Service

Exhibit 1 to Attachment 4

Excerpt from HMRC's "Test for Tax Non-Compliance"

***Condition one**: (An in-scope entity or person)*

1. There is a person or entity ("**X**") which is either:

   1) the Economic Operator or Essential Subcontractor (EOS);

   2) part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1]; or

   3) any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

***Condition two**: (Arrangements involving evasion, abuse or tax avoidance)*

2. X has been engaged in one or more of the following:

   a. fraudulent evasion[2];

   b. conduct caught by the General Anti-Abuse Rule[3];

   c. conduct caught by the Halifax Abuse principle[4];

   d. entered into arrangements caught by a DOTAS or VADR scheme[5];

   e. conduct caught by a recognised 'anti-avoidance rule'[6] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

   f. entered into an avoidance scheme identified by HMRC's published Spotlights list[7]; and/or

   g. engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10

[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions.

[4] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others.

[5] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

[6] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

[7] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight.

Condition three: *(Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))*

3. X's activity in Condition 2 is, where applicable, subject to dispute and/or litigation as follows:

   i. In respect of (a), either X:

      1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[8]; or,

      2. Has been charged with an offence of fraudulent evasion.

   ii. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

   iii. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

   iv. In respect of (f) this condition is satisfied without any further steps being taken.

   v. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

4. For the avoidance of doubt, any reference in this Exhibit 1 (Excerpt from HMRC's "Test for Tax Non-Compliance") to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

[8] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

Crown Commercial Service

Exhibit 2 to Attachment 4

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: *[for Supplier to insert Contract reference number and contract date]* ('**the Agreement**')

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Government Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Government Data provided to me.

SIGNED:	
FULL NAME:	
POSITION:	
COMPANY:	
DATE OF SIGNATURE:	

Crown Commercial Service

Attachment 5 – List of Transparency Reports

Attachment 5 is not applicable – no additional reports are required to the reports referenced in each Delivery SOW of Attachment 7 (Deliverables)

It is agreed that no transparency reports are required to be delivered by the Supplier as the Buyer will have access to relevant information through the governance process applied to all ACS services. A Technical Account Manager ("**TAM**") is allocated to the contract and is responsible for the deliverables as set out in the Order Form and in each Delivery SOW of Attachment 7 (Deliverables). Monthly reporting will provide metrics on the Service Availability Level for Services that the Buyer purchased under its order. There are no Service Availability Level for Oracle Consulting Services.

The TAM will also be able to provide access other information about the ACS services. The types of information tare subject to change but, as at the date of this Order Form, include:

- **Service details** e.g. service status, utilisation & availability,
- **Critical notifications** relating to a customer's services e.g. maintenance notices, incident notifications & root cause assessment information
- **Reports** relating to a customer's services e.g. usage, security assurance statements, audit reports, user experience insight reports

Any services information provided by Supplier will be deemed to be confidential and may be commercially sensitive. Before disclosing any such information to a third party or making such information publicly available, the Buyer must consult with the Supplier and take into account the Supplier's representations relating to such disclosure. Except to the extent required by law, such information will not be published or disclosed without Supplier's prior written consent.

Crown Commercial Service

Attachment 6 – Service Descriptions and Product Terms

SERVICE DESCRIPTIONS:

See the relevant Service Description that may be applicable to the Services purchased and specified under this Order Form above:

- **Oracle Advanced Customer Services (ACS) Service Descriptions, Effective Date: 12-DEC-2022** (deemed to be attached as **Exhibit A** to this Attachment 6 if applicable to any additional Services); and

Oracle Advanced Customer Services (A

Note - see separate file named EHIBIT A Contract (ecm_12598)- Oracle Advanced Customer Services (ACS) Service Descriptions

Copies of the Services Service Descriptions are not attached to this Order Form as they are not applicable to the initial scope of Services set out in Attachment 7. If the Services Service Descriptions are applicable to any additional Services, then copies of such documents will be provided upon request.

The Services Service Descriptions are subject to change from time-to-time, but such changes will not materially reduce the level of performance, security, or availability of the Services under this order for the duration of the Services Period.

PRODUCT TERMS:

The Product Terms are as set in in the "Product Terms – Licence Terms" sub-section below, and in the Applicable Supplier Terms **Exhibit B (Oracle Product Terms)** to this Attachment 6 (Service Descriptions and Product Terms). A copy of the Oracle Product Terms is attached at the end of this Order Form.

Oracle Professional Services Product Term

Product Terms – Licence Terms

Clause 9.4 of the Call Off Contract is applicable subject only to clause 6 of the Product Terms which provides:

"6.1. Your licence to use the Services is limited to Your internal business operations only.

6.2 You may not, and may not cause or permit others to: (a) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish, download, or copy any part of the Services (including data structures or similar materials produced by programs) unless required to be permitted by law for interoperability; (b) access or use the Services to build or support, directly or indirectly, products or services competitive to Oracle; or (c) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Services to any third party except as permitted by this Agreement or Your order."

Crown Commercial Service

Attachment 7 – Deliverables

REDACTED IN FULL FOI 43 & 24

Crown Commercial Service

Attachment 8 – Data Processing Agreement

To protect Your Content (as defined in the Product Terms) provided to the Supplier as part of the provision of the Services, the Supplier will comply with the applicable version of the Data Processing Agreement for Services (the "**Data Processing Agreement**"). The version of the Data Processing Agreement applicable to this Attachment 8 (Data Processing Agreement) of the Order Form is available at https://www.oracle.com/contracts/docs/corporate_data_processing_agreement_062619.pdf?download=false . In the event of any conflict between the terms of the Data Processing Agreement and the terms of the Service Specifications (as defined in the Product terms) (including any applicable Oracle privacy policies), the terms of the Data Processing Agreement shall take precedence.

Crown Commercial Service

Annex 1

Professional Services Call-Off Terms

The Call-Off Terms are the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website https://www.crowncommercial.gov.uk/agreements/RM6292 titled "*RM6292 Professional services template call-off terms v.3.0*" ("**Agreed Call-Off Terms**") and the Agreed Call-Off Terms v.3.0 are incorporated in this Order Form by reference accordingly.

Exhibit B

ORACLE PRODUCT TERMS FOR CCS FRAMEWORK RM6292

ORACLE PROFESSIONAL SERVICES

These Terms represent the Product Terms as envisaged by Framework Contract RM6292 entered into between Oracle and CCS. They form part of a Call Off Contract entered into between Oracle and the Buyer identified in a relevant Order Form pursuant to the above Framework Contract. Words or phrases used in this document which are defined in the Call Off Contract have the same meaning when used in these Product Terms.

1. References in these Product Terms to "**Oracle**" "**we**," "**us**," or "**our**" are references to Oracle Corporation UK Limited and references to You are to the Buyer identified in the Order Form.

2. All Call Off Contracts require the express written agreement of and signature of Oracle on the applicable Order Form. Oracle expressly reserves the right to decline to accept any Order Form (including Direct Awards) if it finds the provisions of the Order Form unacceptable.

3. If, for whatever reason, the Buyer consumes Services in excess of the Contract anticipated annual value specified in the Order Form, the Buyer shall be given the option of suitably increasing the level of the stated Contract anticipated annual value. If the Buyer exercises this option, such excess Services shall be deemed supplied pursuant to the Call Off Contract and charged accordingly. If the Buyer is unwilling or unable to do so for whatever reason, any Services above the stated anticipated annual value shall be deemed to have been supplied by Oracle subject to Oracle's standard terms and conditions in force from time to time related to the Service in question and the price payable shall be that quoted in Oracle's standard price list published at the applicable time for the Services in question (unless the Parties agree otherwise).

4. If, for whatever reason, the Buyer elects to procure services from Oracle which are deemed to be out of scope for procurement under the CCS Framework RM6292, the Buyer shall be deemed to have procured such services subject to Oracle's standard terms and conditions in force from time to time related to the Service in question and the price payable shall be that quoted in Oracle's standard price list published at the applicable time for the Services in question (unless the Parties agree otherwise).

5. THIRD-PARTY CONTENT, SERVICES AND WEBSITES

5.1. You may have access to Third Party Content through use of the Services. Unless otherwise stated in Your order, all ownership and intellectual property rights in and to Third Party Content and the use of such content is governed by separate third party terms between You and the third party.

5.2. The Services may enable You to link to, transfer Your Content or Third Party Content to, or otherwise access, third parties' websites, platforms, content, products, services, and information ("Third Party Services"). Oracle does not control and is not responsible for Third Party Services. You are solely responsible for complying with the terms of access and use of Third Party Services, and if Oracle accesses or uses any Third Party Services on Your behalf to facilitate performance of the Services, You are solely responsible for ensuring that such access and use, including through passwords, credentials or tokens issued or otherwise made available to You, is authorized by the terms of access and use for such services. If You transfer or cause the transfer of Your Content or Third Party Content from the Services to a Third Party Service or other location, that transfer constitutes a distribution by You and not by Oracle. Any Third Party Content we make accessible is provided on an "as-is" and "as available" basis without any warranty of any kind. You acknowledge and agree that we are not responsible for, and have no obligation to control, monitor, or correct, Third Party Content. To the extent not prohibited by law, we disclaim all liabilities arising from or related to Third Party Content.

5.3. You acknowledge that: (i) the nature, type, quality and availability of Third Party Content may change at any time during the Services Period, and (ii) features of the Services that interoperate with Third Party Services such as Facebook™, YouTube™ and Twitter™, etc., depend on the continuing availability of such third parties' respective application programming interfaces (APIs). We may need to update, change or modify the Services under this Agreement as a result of a change in, or unavailability of, such Third Party Content, Third Party Services or APIs. If any third party ceases to make its Third Party Content or APIs available on reasonable terms for the Services, as determined by us in our sole discretion, we may cease providing access to the affected Third Party Content or Third Party Services without any liability to You. Any

changes to Third Party Content, Third Party Services or APIs, including their unavailability, during the Services Period does not affect Your obligations under this Agreement or the applicable order, and You will not be entitled to any refund, credit or other compensation due to any such changes.

6. LICENCE AND DERIVATIVE WORKS

6.1. Your licence to use the Services is limited to Your internal business operations only.

6.2. You may not, and may not cause or permit others to: (a) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish, download, or copy any part of the Services (including data structures or similar materials produced by programs) unless required to be permitted by law for interoperability; (b) access or use the Services to build or support, directly or indirectly, products or services competitive to Oracle; or (c) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Services to any third party except as permitted by this Agreement or Your order.

7. EXCLUSIVE REMEDIES

7.1. We warrant that during the Contract Period we will perform the Services using commercially reasonable care and skill in all material respects as described in the Service Specifications.

7.2. We do not warrant that the services will be performed error-free or uninterrupted, that we will correct all services errors, or that the services will meet your requirements or expectations. We are not responsible for any issues related to the performance, operation or security of the services that arise from your content or third party content or services provided by third parties.

7.3. For any breach of the services warranty in 7.1 above or elsewhere in the call off contract, your exclusive remedy and our entire liability shall be the correction of the deficient services that caused the breach of warranty, or, if we cannot substantially correct the deficiency in a commercially reasonable manner, you may end the deficient services and we will refund to you the fees for the terminated services that you pre-paid to us for the period following the effective date of termination.

7.4. To the extent not prohibited by law, the warranties set out in the call off contract are exclusive and all other warranties or conditions, whether express or implied, are expressly excluded, including, without limitation, for software, hardware, systems, networks or environments or for merchantability, satisfactory quality and fitness for a particular purpose.

7.5. In no event will either party or its affiliates be liable for any consequential, incidental, special, punitive, or exemplary damages, sales, data, data use, goodwill, or reputation.

7.6. The cap on liability in clause 9.4.2 of the Call Off Contract shall only apply in circumstances where there has been unauthorised access to Your Content caused by a breach of Oracle's security practices. All other breaches shall be covered by the cap in clause 9.1 of the Call Off Contract.

7.7. Unless otherwise specified in Your order (including in the Service Specifications), Your Content may not include any sensitive or special data that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Service Specifications. If available for the Services, You may purchase additional services from us (e.g., Oracle Payment Card Industry Compliance Services) designed to address specific data security or data protection requirements applicable to such sensitive or special data You seek to include in Your Content.

7.8. Should Buyer Content become damaged or corrupted, Oracle's obligation to restore the damaged or corrupted data shall be limited to taking the most recent available back-up copy of the data and making that available via the Services.

7.9. The Buyer's rights to retain or set-off amounts owed to it shall only apply where Oracle has agreed that the amount is owed or the Buyer has a binding court judgment to that effect. Otherwise fees payable shall be paid in full and all other rights of set-off whether at common law or otherwise in favour of the Buyer are excluded.

8. IPR INFRINGEMENT

8.1. The indemnity in clause 10.7 of the Call Off Contract shall only apply in respect of damages, liabilities, costs and expenses awarded by the court to the third party claiming infringement or under a settlement agreed to by the indemnifying Party

8.2. If the indemnifying Party believes or it is determined that use of the Services may infringe a third party's intellectual property rights, and if the alternatives set out in clause 10.8 of the Call OffContract are not

commercially reasonable, the indemnifying Party may end the Services associated (or relevant part thereof) and refund any unused, prepaid fees for such Services.

8.3. Oracle will not be liable under the indemnity if the Buyer (a) alters the item in question or uses it outside the scope of use identified in Oracle's user or program documentation or Service Specifications, or (b) uses a version which has been superseded, if the infringement claim could have been avoided by using an unaltered current version which was made available to the Buyer. Oracle will not indemnify You to the extent that an infringement claim is based on Third Party Content or any material from a third party portal or other external source that is accessible or made available to You within or by the Services (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, marketing data from third party data providers, etc.).

8.4. This section 8 (amending clause 10.7- 10.8 of the Call Off Contract) provides the parties' exclusive remedy for any IPR Claims or related damages.

9. SERVICE ANALYSES AND ORACLE SOFTWARE

9.1. We continuously monitor the Services to facilitate Oracle's operation of the Services; to help resolve Your service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. Oracle monitoring tools do not collect or store any of Your Content residing in the Services, except as needed for such purposes. Oracle does not monitor, and does not address issues with, non-Oracle software provided by You or any of Your Users that is stored in, or run on or through, the Services. Information collected by Oracle monitoring tools (excluding Your Content) may also be used to assist in managing Oracle's product and service portfolio, to help Oracle address deficiencies in its product and service offerings, and for license management purposes.

9.2. We may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). We may make Service Analyses publicly available; however, Service Analyses will not incorporate Your Content, Personal Data or Confidential Information in a form that could serve to identify You or any individual. We retain all intellectual property rights in Service Analyses.

9.3. We may provide You with the ability to obtain certain Oracle Software (as defined below) for use with the Services. If we provide Oracle Software to You and do not specify separate terms for such software, then such Oracle Software is provided as part of the Services and You have the non-exclusive, worldwide, limited right to use such Oracle Software, subject to the terms of this Agreement and Your order (except for separately licensed elements of the Oracle Software, which separately licensed elements are governed by the applicable separate terms), solely to facilitate Your use of the Services. You may allow Your Users to use the Oracle Software for this purpose, and You are responsible for their compliance with the license terms. Your right to use any Oracle Software will terminate upon the earlier of our notice (by web posting or otherwise) or the end of the Services associated with the Oracle Software. Notwithstanding the foregoing, if Oracle Software is licensed to You under separate terms, then Your use of such software is governed by the separate terms. Your right to use any part of the Oracle Software that is licensed under the separate terms is not restricted in any way by this Agreement.

10. COMPLIANCE WITH EXPORT LAWS

10.1. Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Services. Such export laws govern use of the Services (including technical data) and any Services deliverables provided under this Agreement, and You and we each agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). You agree that no data, information, software programs and/or materials resulting from the Services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

10.2. Specifically, but without limitation, Services may not be delivered to or accessed by Users in Venezuela, nor may the Services or any output from the Services be used for the benefit of any individuals or entities in Venezuela.

10.3. You acknowledge that the Services are designed with capabilities for You and Your Users to access the Services without regard to geographic location and to transfer or otherwise move Your Content between the Services and other locations such as User workstations. You are solely responsible for the authorization and management of User accounts across geographic locations, as well as export control and geographic transfer of Your Content.

11. ASSIGNMENT BY THE BUYER

Should the Buyer seek to assign the benefit of the Call Off Contract in accordance with its terms, the Buyer will procure that the proposed assignee agrees to execute a form of assignment directly with Oracle (in a form reasonably specified by Oracle) and agrees to abide by the terms of the Call Off Contract and accepts a liability to pay for the Services ordered in accordance with the provisions of the Call Off Contract.

12. BUYER REGULATORY AND LEGAL COMPLIANCE

Prior to entering into an order governed by the Call Off Contract, You are solely responsible for determining whether the Services meet Your technical, business or regulatory requirements. Oracle will cooperate with Your efforts to determine whether use of the standard Services are consistent with those requirements. Additional fees may apply to any additional work performed by Oracle or changes to the Services. You remain solely responsible for Your regulatory compliance in connection with Your use of the Services.

13. TERMINATION BY THE BUYER ON NOTICE WITHOUT CAUSE

Should the Buyer exercise the right to terminate without cause contained in clause 16.1 of the Call Off Contract, the Buyer shall nevertheless be obliged to forthwith pay an amount equal to the Charges that would otherwise have been payable throughout the remainder of the originally committed Contract Period.

14. OFF-BOARDING SERVICES

It is not anticipated that Oracle will be required to provide any Off Boarding Services upon termination or expiry of the Call Off Contract. However, if any such Off Boarding Services are required or are specified in the Order Form then Oracle will be entitled to charge for such Services at a price to be reasonably agreed between the Parties or, in the absence of agreement, at Oracle's standard charge rates applicable at the time for such Services.

15. AUDIT

15.1. Any audit conducted by the Buyer under the Call Off Contract must comply with the provisions of this section 15. Under no circumstances will the scope of an audit include Oracle's costs or profitability (or those of its Sub-Contractors) since access to this information is not necessary in order to verify the accuracy of the Charges.

15.2. You may audit Oracle's compliance with its obligations under the Call Off Contract up to once per year. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

15.3. If a third party is to conduct the audit, 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.

15.4. To request an audit, You must submit a detailed proposed audit plan to Oracle at least two (2) 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.

15.5. 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.

15.6. Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of the Call Off Contract. You may use the audit reports only for the purposes of

meeting Your regulatory audit requirements and/or confirming compliance with the requirements of the Call Off Contract.

15.7. 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 Call Off Contract such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

15.8. 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 (12) 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.

16. FORCE MAJEURE

Nothing in clause 22 of the Call Off Contract excuses Your obligation to continue to pay for the Services.

17. STANDARDS

Please be aware that not all data centres used by Oracle comply with every one of the Standards (as defined). When placing orders via the Supplier Portal it is your responsibility to check with Oracle the applicable compliance status before taking a decision to place the order.

18. DATA PROCESSING

18.1. Where personal data is processed by Oracle as part of the Services, the terms of Oracle's Professional Services Delivery Policy will apply (see **Appendix 2**) as will the Oracle Services Privacy Policy (see **Appendix 3**).

18.2. Oracle has adopted and had approved by relevant regulators a set of Binding Corporate Rules ("**BCRs**") governing the processing of and internal transfers of personal data by Oracle to and from companies within the Oracle Group. These BCRs form part of these Product Terms. The current version of the BCRs (see **Appendix 4**)

19. UPDATES

These Product Terms, the applicable Service Specifications, relevant Service Level Agreements and any documents referenced in any of them may be updated by Oracle from time to time. As and when there is any update to these documents Oracle will take reasonable steps to bring this to your attention. Continued use of the Services will be taken as acceptance of the updates unless you raise valid objections as envisaged by clause 5 of the Call Off Contract within thirty (30) days of being made aware of the update.

20. TUPE

If any individual claims to have transferred to Oracle or a Sub-Contractor upon the commencement of any Service or from Oracle or a Sub-Contractor to the Buyer or any successor provider upon termination of the provision of any Service, the provisions of **Appendix 5 (TUPE)** shall apply.

21. BUYER RESPONSIBILITIES

You will cooperate generally with Oracle to facilitate the provision of the Services and Deliverables on a timely basis including taking decisions promptly and making relevant subject matter experts available on a timely basis. Details of Your obligations and the assumptions in respect of the Services upon which the Charges have been based are as set out in the Oracle's Professional Services Delivery Policy will apply (see **Appendix 2**). Your specific responsibilities and assumptions may in addition be set out or referenced in the Order Form or the implementation plan. Failure by You to comply with the Your responsibilities outlined in this clause shall

constitute a cause that may entitle Oracle to render additional Charges provided that it notifies Your promptly given the circumstances.

22. ADDITIONAL LICENSES AND ORACLE LINUX SUPPORT

Oracle licenses and support are not provided by Oracle under the terms of Framework Agreement RM6292. However, should wish to obtain additional licenses and support in connection with the Oracle Cloud Services, Oracle has therefore agreed that, for all Oracle Cloud Services purchased under the Call Off Contract, the terms set out in **Appendix 6 (Additional Licenses and Oracle Linux Support)** shall apply. By signing the Order Form, You acknowledge that although the licenses and support stated in **Appendix 6 (Additional Licenses and Oracle Linux Support)** will be provided in connection with the Oracle Cloud Services, they do not fall within the scope of the Call-Off Contract and are not subject to the terms and conditions of the Call-Off Contract or Framework Agreement RM6292. You therefore accept that Your use of such licenses and support shall be governed by the terms stated in **Appendix 6 (Additional Licenses and Oracle Linux Support)** notwithstanding anything to the contrary in the Call-Off Contract or Framework Agreement RM6292.

23. DEFINITIONS

23.1. Terms used in these Product Terms shall have the following meanings:

"**Oracle Software**" means any software agent, application or tool that Oracle makes available to You for download specifically for purposes of facilitating Your access to, operation of, and/or use with, the Services. "Program Documentation" refers to the user manuals, help windows, readme files for the Services and any Oracle Software. You may access the documentation online at http://oracle.com/contracts or such other address specified by Oracle.

"**Service Specifications**" means the following documents, as applicable to the Services under Your Order Form: (a) the Oracle Cloud Hosting and Delivery Policies, the Program Documentation, the Oracle service descriptions, and the Data Processing Agreement described in the Call Off Contract; (b) Oracle's privacy policies; and (c) any other Oracle documents that are referenced in or incorporated into Your Order Form. The following do not apply to any non-Cloud Oracle service offerings acquired in Your Order Form, such as professional services: the Oracle Cloud Hosting and Delivery Policies and Program Documentation.

"**Third Party Content**" means all software, data, text, images, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of Oracle that You may access through, within, or in conjunction with Your use of, the Services. Examples of Third Party Content include data feeds from social network services, rss feeds from blog posts, Oracle data marketplaces and libraries, dictionaries, and marketing data. Third Party Content includes third-party sourced materials accessed or obtained by Your use of the Services or any Oracle-provided tools.

"**Users**" has the same meaning as Buyer Users as defined in Schedule 1 to the Call Off Contract.

"**Your Content**" has the same meaning as Buyer Content as defined in Schedule 1 to the Call Off Contract. Services under this Agreement, Oracle Software, other Oracle products and services, and Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the term "Your Content." Your Content includes any Third Party Content that is brought by You into the Services by Your use of the Services or any Oracle-provided tools.

APPENDIX 1 ORACLE PRODUCT TERMS

PROFESSIONAL SERVICES ADDENDUM

This Professional Services Addendum (this "**PS Addendum**") is an addendum to the Product Terms referenced above that provides terms applicable to order for professional services placed under the Call-Off Contract ("**Professional Services**"). Definitions used in the Product Terms shall have the same meaning under this PS Addendum, unless expressly stated otherwise. In the event of a direct conflict between this PS Addendum and the Call-Off Contract, this PS Addendum shall prevail.

1. OWNERSHIP

You or Your licensors retain all ownership and intellectual property rights in and to Your Content. We or our licensors retain all ownership and intellectual property rights in and to the Services, derivative works thereof, and anything developed or delivered by or on behalf of us under this Agreement. In addition to Your rights to Your Content under Section 6 of the Product Terms, You retain all ownership and intellectual property rights to Your confidential and proprietary information that You provide to Oracle in Your order to perform Professional Services.

2. WARRANTY

a. In addition to the warranties in Section 7 of the Product Terms, Oracle warrants that it will perform Professional Services in a professional manner consistent with industry standards. You must notify Oracle of any warranty deficiencies within ninety (90) days from performance of the deficient Professional Services.

b. **FOR ANY BREACH OF THIS PARTICULAR WARRANTY, YOUR EXCLUSIVE REMEDY AND ORACLE'S ENTIRE LIABILITY SHALL BE THE RE-PERFORMANCE OF THE DEFICIENT PROFESSIONAL SERVICES, OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, YOU MAY END THE DEFICIENT PROFESSIONAL SERVICES AND RECOVER THE FEES YOU PAID TO ORACLE FOR THE DEFICIENT PROFESSIONAL SERVICES.**

3. GENERAL INDEMNIFICATION

a. Each Party ("**Indemnitor**") shall defend and indemnify the other Party ("**Indemnitee**") against any and all claimsof bodily injury and tangible personal property damage resulting from grossly negligent or intentionally wrongful actions or omissions of the Indemnitor or a person employed by the Indemnitor (i.e., as an employee or subcontractor) while performing or participating in on-site professional Services under an order, if such actionsor omissions were not proximately caused by the action or omission of the Indemnitee or any third party; provided, however, that the Indemnitee:

i. Notifies the Indemnitor promptly in writing, not later than thirty (30) days after Indemnitee receives noticeof the claim (or sooner if required by law).
ii. Gives the Indemnitor sole control of the defense and any settlement negotiations.
iii. Gives the Indemnitor the information, authority, and assistance the Indemnitor needs to defend against or settle the claim.

b. As used in this section, the term "tangible personal property" shall not include software, documentation, data or data files. The Indemnitor shall have no liability for any claim of bodily injury or tangible personal property damage arising from use of software or hardware. This section states the parties' entire liability and exclusive remedy for bodily injury and property damage.

4. BACKGROUND CHECKS

a. Oracle has implemented background screening procedures for applicants worldwide, subject to local laws, regulations, and customs. Rollout of these procedures was commenced in the various regions as follows: (i) United States – 2003; Canada – 2004; (ii) Europe, the Middle East and Africa – 2004, (iii) Asia Pacific – 2004, and (iv) Latin America – 2006. In general, international transfers and individuals with valid government issued security clearances are not subject to a background check. Further, processing and procedural variances may apply to students/interns, certain university hires, and employees of acquired companies. Oracle confirms that it conducts the following screening procedures in the various jurisdictions as of the date of Your Services Agreement:

i North America (U.S. & Canada)
- Education (highest degree received)
- Employment (up to four employers in the last seven years)
- Criminal record check
- Social Security Trace (U.S. Only)
- Office of Foreign Asset Control Specially Designated Nationals (SDN) screen (U.S. Only)

ii Asia Pacific
- Education (highest degree received)
- Employment (up to four employers in the last seven years)
- Criminal record check (as allowed under local law)

iii Europe, Middle East and Africa (EMEA)
- Education (highest degree received)
- Employment (up to three employers in the last five years)
- Address Check (U.K. only)
- Financial Probity Check (U.K. and South Africa only)

iv Latin America
- Education (highest degree received)
- Employment (up to four employers in the last seven years)
- Criminal record check

b. In addition, all Oracle employees are subject to the following minimum reviews upon hire, in accordance with local legislation:

i Identity
ii Right to work

c. Identity and Right to work reviews are performed separately and independently of any other screenings.

5. ACCEPTANCE OF DELIVERABLES

Where Deliverables are provided under Your Order Form, upon completion of any Deliverable set forth in the Order Form, Oracle shall provide a copy thereof to You. At such time, if You request, Oracle will demonstrate to You that the Deliverable conforms to the description specified for such deliverable in the Order Form. You will be responsible for any additional review and testing of such Deliverable in accordance with any mutually agreed test scripts as may be included in Oracle's project management plan. If the Deliverable does not conform with the description for such Deliverable specified in the Order Form and/or any such test scripts, You shall have three (3) Working Days after Oracle's submission of the Deliverable ("**Acceptance Period**") to give Oracle written notice which shall specify the deficiencies in detail. Oracle shall use reasonable efforts to promptly cure any such deficiencies. After completing such cure, Oracle shall resubmit the Deliverable for Your review and testing as set forth above. Upon accepting any Deliverable submitted by Oracle, You shall provide Oracle with written acceptance of such Deliverable. If You fail to provide written notice of any deficiencies within the Acceptance Period, as provided above, such deliverable shall be deemed accepted at the end of the Acceptance Period.

6. TERMS IN YOUR ORDER FORM

In addition to setting forth the scope of Professional Services in Your order, You and Oracle may agree upon additional or different terms and conditions in such an order, including, for example, with respect to Your cooperation, project assumptions, fees, expenses, and taxes.

APPENDIX 2 ORACLE PRODUCT TERMS

ORACLE'S PROFESSIONAL SERVICES DELIVERY POLICY

These Professional Services Delivery Policies ("Policies") apply to the consulting services, advanced customer services, and managed services You ordered ("Services"). These Policies do not apply to Oracle Cloud Services. Oracle may update these Policies and the documents referenced herein; however, Oracle updates will not result in a material reduction in the level of performance, functionality, security, or availability of the Services, or in a material increase in the level of Your cooperation, for the duration of Your order.

ON-SITE SERVICES

You and Oracle must agree upon the performance of the Services at one of Your facilities, taking into consideration all applicable laws, regulations, standards, and protocols. If agreed upon, You must provide a safe and healthy workspace for all Oracle resources (e.g., free from recognized hazards that cause, or are likely to cause, serious physical harm or death, and with acceptable ventilation, oxygen concentration and sound levels, and ergonomically correct workstations).

If the performance of on-site Services becomes negatively impacted due to a declared disaster, public health or safety concern, or national or global emergency, Oracle and You shall cooperate in good faith to review such impact and, if necessary, invoke the change control process.

If requested, Oracle resources will obtain a badge to enter Your facilities and comply with Your reasonable physical security and safety policies and procedures while on-site, to the extent they do not violate any applicable law (including privacy laws), place Oracle resources in harm, or require Oracle resources to undergo background checks or other screening (unless set forth in Your order). However, no terms included in any such policies and procedures shall modify the Services, and You shall provide training regarding such policies and procedures as requested.

NETWORK ACCESS

If You and Oracle agree that the Services will be performed remotely, You shall provide remote access to Your systems and environments to enable Oracle to perform such Services, using an Oracle-defined virtual private network, Oracle FastConnect (or similar Oracle technology), or the Oracle Web Conference or other agreed-upon, third-party web conferencing application (collectively, "remote access tools").

You are responsible for installing the remote access tools prior to the commencement of the Services and maintaining them throughout the Services (e.g., by acquiring any equipment and performing labor) to enable Oracle to perform the Services.

Oracle is not responsible for any network connections or related problems, or for Your failure to provide remote access to Your systems and environments.

THIRD-PARTY COLLABORATION TOOLS

If You and Oracle agree, Oracle will provide You with access to third-party tools (e.g., Confluence or Jira) to promote collaboration related to the Services (each, a "collaboration tool"). Upon such access, You agree to:

- Only use a collaboration tool in connection with the Services, and cease use upon the end of the Services or written notice by Oracle, whichever is earlier.
- Promptly notify Oracle when You authorize an individual to use a collaboration tool and when You revoke such authorization due to reassignment, resignation, or termination.
- Do not store source code or product, security, financial, personal, or production data in a collaboration tool.
- Comply with the terms of service for a collaboration tool; specifically, for Wrike at https://www.wrike.com/security/terms/; and for Atlassian (as a "Secondary User") at https://www.atlassian.com/legal/software-license-agreement.

A collaboration tool is offered on an "as is" and "as available" basis without any warranty, express or implied, or indemnity or liability.

YOUR COOPERATION

Oracle's ability to perform the Services depends upon You providing the cooperation listed below and in Your order and as agreed upon during the Services (collectively, "cooperation"):

1. For Services related to Oracle Cloud Services, obtain and maintain the Oracle Cloud Services under separate contract prior to and during the Services.

2. For all other Services: (a) obtain licenses for all applicable Products under separate contract prior to the commencement of the Services; (b) maintain the properly configured hardware/operating system platform to support the Services; and (c) maintain annual technical support for all such Products with access to software patches and updates made available by Oracle under separate contract during the Services.

3. Provide information, data, and documentation agreed upon for the Services.

4. Allocate agreed-upon functional, technical, and business resources, including from Your third parties, with the skills and knowledge to support the performance of the Services.

5. Provide the rights for Oracle to use, on Your behalf, any agreed-upon third-party products that are part of Your system or used to perform the Services.

6. Provide notices and obtain consents agreed upon for Oracle to perform the Services.

If You fail to provide reasonable cooperation, Oracle will not be responsible for any resulting deficiency in performing the Services.

PRIVACY AND SECURITY

In performing the Services, Oracle will comply with the following documents (which are incorporated herein):

- Oracle Services Privacy Policy attached at Appendix 3 to the Product Terms.

- Oracle Data Processing Agreement for Oracle Services, available at https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data- processing and at Attachment 8 to the Order Form.

- Oracle Corporate Security Practices, available at https://www.oracle.com/assets/corporate-security-practices-4490843.pdf.

- Oracle Consulting & Advanced Customer Services Security Practices, available at https://www.oracle.com/corporate/contracts/consulting/policies.html.

SUBCONTRACTORS

Oracle may use subcontractors to support its performance of the Services, subject to any applicable terms and conditions in Your Master Agreement or order; provided that Oracle is responsible for its subcontractors' performance to the same extent as its employees' performance.

CHANGE CONTROL PROCESS

All requests for proposed changes to the Services must be in writing, including those related to changes in scope, deliverables, Your cooperation, project assumptions, or any other aspect of Your order.

Oracle shall not be obligated to perform, and You shall not be obligated to pay for, tasks related to any such changes unless agreed upon in an amendment to Your Order Form.

APPENDIX 3 ORACLE PRODUCT TERMS

ORACLE SERVICES PRIVACY POLICY

I. SERVICES PERSONAL INFORMATION DATA PROCESSING TERMS

Oracle treats all Services Personal Information in accordance with the terms of Sections I and III of this Policy and Your order for Services.

In the event of any conflict between the terms of this Services Privacy Policy and any privacy terms incorporated into Your order for Services, including an Oracle Data Processing Agreement, the relevant privacy terms of Your order for Services shall take precedence.

1. Performance of the Services

Oracle may process Services Personal Information for the processing activities necessary to perform the Services, including for creating an Oracle services account to access Oracle products and services, for testing and applying new product or system versions, patches, updates and upgrades, and resolving bugs and other issues You have reported to Oracle.

2. Customer instructions

You are the controller of the Services Personal Information processed by Oracle to perform the Services. Oracle will process your Services Personal Information as specified in Your Services order and Your documented additional written instructions to the extent necessary for Oracle to (i) comply with its processor obligations under applicable data protection law or (ii) assist You to comply with Your controller obligations under applicable data protection law relevant to Your use of the Services. Oracle will promptly inform You if, in our reasonable opinion, Your instruction infringes applicable data protection law. You acknowledge and agree that Oracle is not responsible for performing legal research and/or for providing legal advice to You. Additional fees may apply.

3. Rights of individuals

You control access to Your Services Personal Information by Your end users, and Your end users should direct any requests related to their Services Personal Information to You. To the extent such access is not available to You, Oracle will provide reasonable assistance with requests from individuals to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to processing of Services Personal Information on Oracle systems. If Oracle directly receives any requests or inquiries from Your end users that have identified You as the controller, we will promptly pass on such requests to You without responding to the end user.

4. Security and confidentiality

Oracle has implemented and will maintain technical and organizational measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Services Personal Information. These measures, which are generally aligned with the ISO/IEC 27001:2013 standard, govern all areas of security applicable to the Services, including physical access, system access, data access, transmission, input, security oversight, and enforcement.

Oracle employees are required to maintain the confidentiality of personal information. Employees' obligations include written confidentiality agreements, regular training on information protection, and compliance with company policies concerning protection of confidential information.

See additional details regarding the specific security measures that apply to the Services are set out in the security practices for these Services, including regarding data retention and deletion, available for review.

5. Incident Management and data breach notification.

Oracle promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or handling of Services Personal Information.

If Oracle becomes aware and determines that an incident involving Services Personal Information qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Services Personal Information transmitted, stored or otherwise processed on Oracle systems that compromises the security, confidentiality or integrity of such Services Personal Information, Oracle will report such breach to You without undue delay.

As information regarding the breach is collected or otherwise reasonably becomes available to Oracle and to the extent permitted by law, Oracle will provide You with additional relevant information concerning the breach reasonably known or available to Oracle.

6. Subprocessors

To the extent Oracle engages Oracle affiliates and third party subprocessors to have access to Services Personal Information in order to assist in the provision of Services, such subprocessors shall be subject to the same level of data protection and security as Oracle under the terms of Your order for Services. Oracle is responsible for its subprocessors' compliance with the terms of Your order for Services.

Oracle maintains lists of Oracle affiliates and subprocessors that may process Services Personal Information.

7. Cross-border data transfers

Oracle is a global corporation with operations in over 80 countries and Services Personal Information may be processed globally as necessary in accordance with this policy and other relevant privacy terms specified applicable to Your Services. If Services Personal Information is transferred to an Oracle recipient in a country that does not provide an adequate level of protection for personal information, Oracle will take adequate measures designed to protect the Services Personal Information, such as ensuring that such transfers are subject to the terms of the EU Standard Contractual Clauses or other adequate transfer mechanism as required under relevant data protection laws.

In the event the Services agreement between You and Oracle references the Oracle Data Processing Agreement for Oracle Services ("DPA"), further details on the relevant data transfer mechanism that applies to Your order for Oracle services are available in the DPA. In particular, for Services Personal Information transferred from the European Economic Area ("EEA") or Switzerland, such transfers are subject to Oracle's Binding Corporate Rules for Processors (BCR-P) or the terms of the EU Standard Contractual Clauses. For Services Personal Information transferred from the United Kingdom (UK), such transfers are subject to the UK Addendum or other appropriate transfer mechanism.

8. Audit rights

To the extent provided in your order for Services, You may at Your sole expense audit Oracle's compliance with the terms of this Services Privacy Policy by sending Oracle a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. You and Oracle will work cooperatively to agree on a final audit plan.

The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to Oracle's on-site policies and regulations, and may not unreasonably interfere with business activities. If You would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle. Upon

completion of the audit, You will provide Oracle with a copy of the audit report, which is classified as confidential information under the terms of Your agreement with Oracle.

Oracle will contribute to such audits by providing You with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services. If the requested audit scope is addressed in a SOC 1 or SOC 2, 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. Additional audit terms may be included in Your order for Services.

9. Deletion or return of Services Personal Information

Except as otherwise specified in an order for services or required by law, upon termination of services, Oracle will return or delete any remaining copies of Your production customer data, including any Services Personal Information, located on Oracle systems or Services environments. Additional information on data deletion functionality is provided in the applicable Services descriptions.

II. SYSTEMS OPERATIONS DATA PROCESSING TERMS

1. Responsibility and purposes for processing personal information

Oracle Corporation and its affiliated entities are responsible for processing personal information that may be incidentally contained in Systems Operations Data in accordance with Sections II and III of this Policy. See the list of Oracle entities. Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country.

We may collect or generate Systems Operations Data for the following business purposes:

- a) to help keep our Services secure, including for security monitoring and identity management;
- b) to investigate and prevent potential fraud or illegal activities involving our systems and networks, including to prevent cyber-attacks and to detect bots;
- c) to administer our back-up disaster recovery plans and policies;
- d) to confirm compliance with licensing and other terms of use (license compliance monitoring);
- e) for research and development purposes, including to analyze, develop, improve and optimize our Services;
- f) to comply with applicable laws and regulations and to operate our business, including to comply with legally mandated reporting, disclosure or other legal process requests, for mergers and acquisitions, finance and accounting, archiving and insurance purposes, legal and business consulting and in the context of dispute resolution.

Where relevant, our legal basis for processing Your personal information is as follows:

- Oracle will process Systems Operations Data as may be necessary to help keep our Services secure; to investigate and prevent potential fraud or illegal activities involving our systems and networks; to administer our back-up disaster recovery plans and policies; and to confirm compliance with licensing and other terms of use.
- Oracle will process Systems Operations Data as may be necessary for internal research for technological development and demonstration and to improve, upgrade, or enhance Oracle products and services based on our legitimate interests when such processing has a limited privacy impact on the individual.
- Oracle may also process Systems Operations Data as necessary for compliance with our legal obligations and for required business operations as noted above.

2. Sharing personal information

Personal information contained in Systems Operations Data may be shared throughout Oracle’s global organization for Oracle’s business purposes. A list of Oracle entities is available as indicated above.

We may also share such personal information with the following third parties:

- third-party service providers (for example IT service providers, lawyers and auditors) in order for those service providers to perform business functions on behalf of Oracle;
- relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings);
- as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

When third parties are given access to personal information contained in Systems Operations Data, we will take the appropriate contractual, technical and organizational measures to ensure, for example, that personal information is only processed to the extent that such processing is necessary, consistent with this Privacy Policy and in accordance with applicable law. Oracle does not share or sell Systems Operations Data subject to this Privacy Policy with third parties for any commercial purposes.

3. Cross-border data transfers

If personal information contained in Systems Operations Data is transferred to an Oracle recipient in a country that does not provide an adequate level of protection for personal information, Oracle will take measures designed to adequately protect information about Users, such as ensuring that such transfers are subject to the terms of the EU Standard Contractual Clauses or other adequate transfer mechanism as required under relevant data protection laws.

4. Security

Oracle has implemented appropriate technical, physical and organizational measures in accordance with the Oracle Corporate Security Practices designed to protect personal information against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

5. Individual rights

To the extent personal information about You is contained in Systems Operations Data, You may request to access, correct, update or delete personal information contained in Systems Operations Data in certain cases, or otherwise exercise Your choices with regard to Your personal information by filling out an inquiry form. We will respond to your request consistent with applicable law.

If are a California resident, under the California Consumer Privacy Act (CCPA), as amended, You may request that Oracle:

1. Discloses to you the following information:

   - the categories and specific pieces of personal information we collected about You and the categories of personal information we sold, if applicable;
   - the categories of sources from which we collected such personal information;
   - the business or commercial purpose for collecting or selling personal information; and
   - the categories of third parties to whom we sold or otherwise disclosed personal information, if applicable.

2. deletes personal information we collected about You or corrects inaccurate personal information about You, unless retained solely for legal and compliance purposes and as otherwise set out in the CCPA.

3. fulfils your request to opt-out of any future sale of personal information about You, if applicable.

If You are an authorized agent making an access or deletion request on behalf of a California resident, please reach out to us via the inquiry form and indicate that You are an authorized agent. We will provide You with instructions on how to submit a request as an authorized agent on behalf of a California resident.

If you submit a request, please be specific as to what right you are asserting (e.g., access, correction, etc.) and which specific pieces of personal information are in scope of your request. In some cases, in order to comply with applicable law or a legal obligation, Oracle may deny your request or may seek more information from you in order to respond to your request.

If You are a California resident, you may obtain information about exercising your rights, as described above, by contacting us at 1-800-633-0748. For information on the CCPA requests Oracle received, complied with, or denied for the previous calendar year, please visit Oracle's Annual Consumer Privacy Reporting page.

III. COMMUNICATIONS AND NOTIFICATIONS TO CUSTOMERS AND USERS

1. Legal requirements.

Oracle may be required to provide access to Services Personal Information and to personal information contained in Systems Operations Data as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect Your or a User's safety or the safety of others, investigate fraud, or respond to government requests, including public and government authorities outside Your or a User's country of residence, for national security and/or law enforcement purposes.

Oracle will promptly inform You of requests to provide access to Services Personal Information, unless otherwise required by law.

2. Global Data Protection Officer

Oracle has appointed a Global Data Protection Officer who is also Oracle's Chief Privacy Officer. If You or a User believe that personal information has been used in a way that is not consistent with this Privacy Policy, or if You or a User have further questions, comments or suggestions related to Oracle's handling of Services Personal Information or personal information contained in Systems Operations Data, please contact the Data Protection Officer by filling out an inquiry form.
Written inquiries to the Global Data Protection Officer may be addressed to:

Oracle Corporation
Global Data Protection Officer
Willis Tower
233 South Wacker Drive
45th Floor
Chicago, IL 60606
U.S.A.

For personal information collected INSIDE the EU/EEA, You may contact Oracle's external EU Data Protection Officer by filling out the inquiry form and selecting "Other Privacy Inquiry - Contact our DPO" in our drop down box or by written inquiry to.

REDACTED FOI 40
Hauptstraße 4
D-85579 Neubiberg / München
Germany
For personal information collected INSIDE Brazil, written inquiries to the Brazilian Data Protection Officer may be addressed to:

REDACTED FOI 40
Rua Dr. Jose Aureo Bustamante, 455
Vila São Francisco
São Paulo, BR

3. Filing a complaint

If You or a User have any complaints regarding our compliance with our privacy and security practices, please contact us. We will investigate and attempt to resolve any complaints and disputes regarding our privacy practices. Users also have the right to file a complaint with a competent data protection authority if they are a resident of a European Union member state.

4. Changes to this Services Privacy Policy

This Privacy Policy was last updated on December 23, 2022. However, the Services Privacy Policy can change over time, for example to comply with legal requirements or to meet changing business needs.

.

APPENDIX 4 TO ORACLE PRODUCT TERMS

ORACLE ADOPTED BCRs

Privacy Code for Processing Personal Information of Customer Individuals

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 expresses Oracle's commitment to conduct our business in accordance with high ethical standards and in accordance with applicable laws and Oracle policies, including the protection of Personal Information. This Privacy Code for Processing Personal Information of Customer Individuals ("**Processor Code"**) specifies how this commitment shall be implemented with respect to Personal Information.

Article 1 – Scope, Applicability and Implementation

Scope – Oracle as Processor	**1.1**	This Processor Code applies to Personal Information of Customer Individuals subject to EEA Data Protection Laws and Processed by Oracle on behalf of its Customers in its role as a Processor in the course of delivering Services.
Electronic and paper-based Processing	**1.2**	This Processor Code applies to the Processing of Personal Information by Oracle by electronic means and in systematically accessible paper-based filing systems.
Sub-policies and notices	**1.3**	Oracle may supplement this Processor Code through sub-policies and notices that are consistent with this Processor Code.
Compliance Responsibility	**1.4**	This Processor Code is binding on Oracle. The Responsible Line of Business Executive shall be accountable for his/her business organization's compliance with this Processor Code. Oracle Staff must comply with this Processor Code.
Effective date	**1.5**	This Processor Code enters into force as of June 26, 2019. The Processor Code (including a list of the Group Companies that may be involved in Processing of Personal Information,) will be published on the Oracle Internet site.

Processor Code supplements prior policies

1.6 This Processor Code supplements all Oracle privacy policies that exist on the Effective Date.

Implementation

1.7 This Processor Code shall be implemented within Oracle based on the timeframes specified in Article 15.

Role of Oracle EMEA

1.8 Oracle Corporation has tasked Oracle EMEA with the coordination and implementation of this Processor Code.

Advice Privacy Professional

1.9 Where there is a question as to the applicability of this Processor Code, Staff shall seek the advice of the appropriate Privacy Professional prior to the relevant Processing.

Article 2 – Services Contract

Services Contract

2.1 Oracle shall Process Personal Information only on the basis of a validly entered into written or electronic services contract with a Customer (**Services Contract**), which complies with EEA Data Protection Law

The Oracle Contracting Entity may use Sub-processors, both Oracle Sub-Processors and Third Party Sub-processors, in the regular performance of Services Contracts. The Services Contract shall authorize the use of such Sub-processors, provided that the Oracle Contracting Entity remains liable to the Customer for the performance of the Services Contract by the Sub-processors in accordance with the terms of the Services Contract. Article 7 shall apply if the Services Contract explicitly authorizes the use of Third Party Sub-processors.

Termination of the Services Contract

2.2 Upon termination of the Services Contract, Oracle shall fulfill its obligations to the Customer in the Services Contract with regard to:

(i) returning Personal Information, including by providing data retrieval functionality (such as the ability to download Personal Information) where available for the relevant Services; or
(ii) promptly deleting any remaining copies of Personal Information in accordance with the Services Contract and, upon the Customer's request, confirm that it has done so.

Audit of termination measures

2.3 Upon termination, Oracle shall, at the request of the Customer, allow for its Processing facilities to be audited in accordance with Articles 10.2, 10.3 and 10.4 (as applicable) to verify that Oracle has complied with its obligations under Article 2.2.

Article 3 – Compliance obligations Oracle

Instructions of the Controller

3.1 Oracle shall Process Personal Information only on behalf of the Customer and in accordance with any instructions received from the Customer consistent with the terms of the Services Contract.

Compliance with Applicable Law

3.2 Oracle shall Process Personal Information only in accordance with the Applicable Processor Law and shall deal promptly and appropriately with requests for assistance of the Customer as reasonably required to ensure compliance of the Processing of Personal Information with its obligations under the Applicable Controller Law in accordance with the Services Contract.

Notification of non-compliance, substantial adverse effect

3.3 If Oracle:

(i) determines that it is unable for any reason to comply with its obligations under Articles 3.1 and 3.2 and Oracle cannot cure this inability to comply; or

(ii) becomes aware of any circumstance or change in the Applicable Processor Law, except with respect to the Mandatory Requirements, or an instruction of the Customer, that is likely to have a substantial adverse effect on Oracle's ability to meet its obligations under Articles 3.1, 3.2 or 10.2;

Oracle shall promptly notify Oracle EMEA and the Customer thereof, in which case the Customer will have the right to temporarily suspend the rel- evant Service(s) under this Processor Code to Oracle 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 shall have the right to terminate the relevant Service(s) in accordance with the terms of the Services Contract.

Request for disclosure of Personal Information

3.4 If Oracle receives a request for disclosure of Personal Information from a law enforcement authority, state security body or other governmental authority (**Authority**), it will first assess on a case-by-case basis whether this request

(**Disclosure Request**) is legally valid and binding on Oracle. Any Disclosure Request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law.

Subject to the following paragraph, Oracle shall promptly inform the Customer, the Lead SA and the Customer SA of any legally valid and binding Disclosure Requests, and will request the Authority to put such Disclosure Requests on hold for a reasonable delay in order to enable the Lead SA to issue an opinion on the validity of the relevant disclosure.

If the suspension and/or 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 Authority to waive this prohibition and will document that it has made this request. In any event, 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.

Inquiries of the Customer

3.5 Oracle shall deal promptly and appropriately with inquiries of the Customer related to the Processing of the Personal Information pursuant to the terms of the Services Contract.

Article 4 – Processor purposes and Description of Processing

Processor Purposes

4.1 As a Processor, Oracle may Process Personal Information 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 or regulation (e.g., data processing law);

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

Description of Processing

4.2 Depending on the relevant Services, Oracle may Process some or all of 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; goods and services provided;
(v) unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

Oracle may Process Personal Information related to some or all of 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

Article 5 – Security Requirements

Data security 5.1 Oracle has implemented and will maintain appropriate technical, physical and organizational measures. These measures take into account the nature, scope and purposes of Processing as specified in this Processor Code and are designed to protect Personal Information from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing. Oracle shall in any event implement and maintain the Corporate Security Pratices specified in Annex 2 of this Processor Code, which may be revised by Oracle, provided that such changes do not in any material manner diminish the level of security provided for under this Processor Code.

Data access and confidentiality

5.2 Oracle shall provide Oracle Staff access to Personal Information only to the extent necessary to perform the Processing. Oracle shall impose confidentiality obligations on Staff that has access to Personal Information.

Reporting of unauthorized access Processing

5.3 Where Oracle Global Information Security becomes aware and determines that Personal Information has been subject to unauthorized Processing (including by an Oracle employee) that compromises the confidentiality, integrity or availability of such Personal Information ("**Personal Information Breach**"), Oracle will report such Personal Information Breach without undue delay to the Customer to the extent permitted by applicable law. Additional details regarding the reporting process and details regarding the Personal Information Breach are specified in the Services Contract.

Article 6 – Transparency to Customer Individuals

Other Requests of Customer Individuals

6.1 Oracle shall promptly notify the Customer of requests or complaints that are received directly from a Customer Individual without responding to such requests or complaints. If Oracle receives such a request or complaint from a Customer Individual, Oracle will refer the Customer Individual to the Customer to address the request or complaint.

Article 7 – Third Party Sub-processors

Third Party Sub-processing Contracts

7.1 Third Party Sub-processors may Process Personal Information only if the Third Party Sub-processor has a binding contract with Oracle. The contract shall impose the same level of data protection and security-related Processing terms on the Third Party Sub-processor as those imposed on the Oracle Contracting Entity by the Services Contract and this Processor Code.

Publication of Lists of Third Party Sub-processors

7.2 Oracle shall publish and maintain on the appropriate Oracle website or online support portal lists of the Third Party Sub-processors involved in the performance of the relevant Services. This overview shall be regularly updated to reflect changes.

Notification new Third Party Sub-processors and right to object

7.3 Oracle shall provide the option to Customers to be notified of any intended changes to the lists of Third Party Sub-processors engaged by Oracle for the delivery of the Services. Within fourteen calendar days of the Customer receiving such notice, the Customer may object to the involvement of such Third Party Sub-processor in the delivery of the Services, providing objective justifiable grounds related to the ability of such Third Party Sub-processor to protect Personal Information or comply with applicable data protection or security requirements. 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 Third Party Sub-processors' compliance or making the Services available without the involvement of such Third Party Sub- processor. To the extent the parties cannot reach a mutually acceptable solution within a reasonable timeframe, the Customer shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (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. If the termination in accordance with this Section 7.3 only pertains to a portion of the Services under a Services Contract, Oracle and Customer will enter into an amendment or replacement contract to reflect such partial termination.

Article 8 – Supervision and compliance

Global Data Protection Officer

8.1 Oracle Corporation has appointed a Global Data Protection Officer who is responsible for:

(i) developing, reviewing and updating Oracle's privacy policies, procedures, system information and training an awareness programs (as required by Article 9);

(ii) supervising and ensuring compliance with this Processor Code;

(iii) providing the annual report (as required by Article 10.5) and periodic reports, as appropriate, to Oracle's General Counsel on data protection risks and compliance issues; overseeing the collection, investigation and resolution of privacy inquiries, concerns and complaints;

(iv) coordinating official investigations or inquiries into the Processing of Personal Information by a public authority;

(v) determining and updating appropriate sanctions for violations of this Processor Code (e.g., disciplinary standards) in co-operation with

other relevant internal functions, such as HR and Legal; and

(vi) Maintaining a fully updated list of the Group Companies and keep track and records of updates to this Processor Code.

Privacy Office

8.2 The Global Data Protection Officer has established and heads Oracle's Privacy Office, consisting of a global network of Privacy Professionals sufficient to direct compliance with this Processor Code within their respective regions or countries.

The Privacy Office performs at least the following tasks:

(i) regularly advising es 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 9.2);

(iii) Implementing the privacy compliance framework (as developed by the Privacy Office in accordance with Article 9);

(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.

Responsible Line of Business Executive

8.3 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 9);

(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 Office to comply with task listed in Article 8.3 sub (ii);

(iii) ensuring that Personal Information is returned or securely deleted upon termination of the Services Contract (as required by Article 2.2);

(iv) consulting with the Privacy Office whenever there is a conflict between

the Processor Code and applicable law (as required by Article 13.1);

(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 this Processor Code (as required by Article 13.2).

Privacy Professionals with statutory position

8.4 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.

Article 9 – Policies, procedures and training

Policies and procedures

9.1 Oracle shall develop and implement policies and procedures to comply with this Processor Code.

System information

9.2 Oracle shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Information (e.g., inventory of systems and processes, privacy impact assessments). A copy of this information will be provided to the Lead SA or to a Customer SA upon request.

Staff training

9.3 Oracle shall provide training on the obligations and principles laid down in this Processor Code and other privacy and data security obligations to Staff that has access to, handles, or has responsibilities associated with managing Personal Information.

Article 10 – Monitoring compliance

Internal audits

10.1 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 this Processor Code, including methods of ensuring that corrective actions will take place. The audits shall be carried out in the course of the regular activities of the BA&A organization or at the request of the Global Data Protection Officer or the General Counsel. The Global Data Protection 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 Global Data Protection Officer, the General Counsel and the Privacy Office shall be informed of the results of the audits. Any violations of this Processor Code identified in the audit report will be reported to the Responsible Line of Business Executive. A copy of the audit results related to compliance with this Processor Code will be provided to the Lead SA or the Customer SA upon request.

Customer audit

10.2 Oracle shall, at its option, either:

(i) make the data center facilities or systems it uses for the Processing of Personal Information available 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 laid down in this Processor Code.

SA audit

10.3 Subject to Article 10.4, the Lead SA may request an audit of the facilities used by Oracle for the Processing of Personal Information for compliance with this Processor Code. In addition, a SA that has the right to audit a Customer (a "**Customer SA**") will be authorized to audit the relevant data transfer for compliance with this Processor Code, subject to the same conditions (regarding the existence of the right to audit, scope, subject and other requirements) as would apply to an audit by that SA of the Customer itself under the Applicable Controller Law.

SA audit procedure

10.4 If a SA requests an audit based on Article 10.3, the following procedure will be followed:

(i) Information sharing: the Customer (or Oracle if the audit is requested by the Lead SA) will attempt to resolve the request using alternative methods of providing information to the SA including Oracle or third party audit or security reports, discussion with Oracle subject matter experts, and review of security, privacy, and operational controls in place. The Customer will have access to its Personal Information in accordance with the Services Contract and may delegate such access to representatives of the SA.

(ii) Examinations: If the SA determines that the information available through these mechanisms is insufficient to address the SA's stated objectives, and upon the Customer's written confirmation that the SA has supervisory authority over the Customer to make such a request, Oracle will provide the SA with the opportunty to communicate with Oracle's auditor at the Customer's expense and if required, a direct right to examine Oracle's data processing facilities used to process the Personal Information on giving reasonable prior notice and during business hours, subject to Oracle's confidentiality policies designed to protect Oracle and other Oracle customer assets.

(iii) Scope: The SA can only access Personal Information belonging to the Customer. The Customer will be liable for Oracle's reasonable additional costs associated with such examination. For clarity, Oracle and its Customers are committed to working together in good faith to resolve a SA request through discussion and interaction among the Customer, Oracle, and the SA.

Annual Report **10.5** The Global Data Protection Officer shall produce an annual Personal Information protection report for the General Counsel on Oracle's compliance with this Processor Code and other relevant issues.

Mitigation **10.6** Oracle shall, if so indicated, ensure that adequate steps are taken to address breaches of this Processor Code identified during the monitoring or auditing of compliance pursuant to this Article 10.

Article 11 – Legal issues

Rights of Customer Individuals **11.1** If Oracle violates the Processor Code with respect to Personal Information of a Customers Individual (**Affected Individual**) and the Affected Individual has a claim against the Customer under Applicable Controller Law with re-

spect to such violation but is unable to enforce the claim against the Customer because: (i) the Customer has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the legal obligations of the Customer by contract or by operation of law (in which case the Affected Individual should enforce its rights against such successor entity), the Affected Individual can enforce as third party beneficiary against the Oracle Contracting Entity any claim as a result of Oracle's breach of Articles 1.5, 2.1, 2.2, 3, 5, 6.1, 7.1, 7.3, 10.2, 10.3, 11.1, 11.2, 11.3, 11.4, 11.7, 11.8 and 13.3.[1]

To the extent the Affected Individual may enforce any such rights against the Oracle Contracting Entity, the Oracle Contracting Entity may not rely on a breach by a Subprocessor of its obligations to avoid liability except to the extent any defense of 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.

Complaints Procedure

11.2 Affected Individuals may file a written (including by email) complaint in respect of any claim they have under Article 11.1 with the Privacy Office. Affected Individuals may also file a complaint or claim with the SAs or the courts in accordance with Article 11.3.

The Privacy Office shall be responsible for handling such complaints. Each complaint will be assigned to an appropriate Staff member (either within the Privacy Office or within the applicable business unit or functional area). The appropriate 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 calandar month of receipt of the complaint. The response will be in writing and will be sent to the Affected Individual via the means that the Affected

[1] Substantially revised due to WP257

Individual originally used to contact Oracle (e.g., via mail or email). 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 in response to the complaint.

In the event that Oracle cannot reasonably complete its investigation and response within one calandar month, it shall inform the Affected Individual within one calendar month of receipt of the compliant that the investigation is ongoing and that a response will be provided within the next two calandar months starting at the end of the first calendar month.

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 11.2, the Affected Individual can file a complaint or claim with the authorities or the courts in accordance with Article 11.3.

Jurisdiction for Claims of Customer Individuals

11.3 The Affected Individual may, at his/her choice, submit any claim under Article 11.1 to against the Oracle Contracting Entity:

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

(ii) the SA in the country of his/her habitual residence, place of work or place where the infringement took place against the Oracle Contracting Entity; or

(iii) the courts in the country of his/her habitual residence, or the country of origin of the data transfer under this Processor Code, against the Oracle Contracting Entity.

The courts and SAs 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.

Available remedies, limitation of damages, burden of proof re. damages for Customer Individuals

11.4 In case an Affected Individual has a claim under Article 11.1, such Affected Individuals shall be entitled to compensation of actual direct damages. However, the Oracle Contracting Entity or Oracle EMEA shall be liable only for actual direct damages (which exclude, without limitation, any indirect, incidental, special, punitive or consequential damages or any lost profits or revenue, lost turnover, cost of capital, downtime cost, and loss of data) suffered by an Affected Individual resulting from a violation of this Processor Code.

Regarding the burden of proof in respect of such damages, it will be for the

Affected Individual to demonstrate that he/she has suffered actual direct damages and to establish facts which show that the damage has occurred because of a violation of this Processor Code. It will subsequently be for the Oracle Contracting Entity or Oracle EMEA to prove that the damages suffered by the Affected Individual due to a violation of this Processor Code are not attributable to a Group Company or a Subprocessor or to assert other applicable defenses.

Rights of Customers

11.5 The Customer may enforce this Processor Code 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 this Processor Code 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.

Available remedies, limitation of damages, burden of proof re. damages for Customers

11.6 In case of a violation of this Processor Code, Customers shall be entitled to compensation of damages consistent with the Services Contract.

Mutual assistance Group Companies and redress

11.7 All Group Companies shall cooperate and assist each other to the extent reasonably possible to achieve compliance with this Processor Code, including an audit or inquiry by the Customer or a SA competent for Customer.

The Oracle Group Company receiving a request for information pursuant to Article 6.1 or a claim pursuant to Article 11.1, is responsible for promptly informing the Privacy Office thereof and handling any communication with the Customer Individual regarding his request or claim as instructed by the Privacy Office.

The Oracle Group Company that is responsible for the Processing to which the request or claim relates, shall bear all costs involved and reimburse any costs made by other Oracle Group Companies in respect thereof upon request.

Advice by Lead SA, decisions other

11.8 Oracle shall abide by the advice of the Lead SA issued on interpretation and application of this Processor Code. Oracle shall abide by a binding decision

Data Protection Authorities of the SA competent for the Customer as instructed by Customer in accordance with Articles 3.2 and 3.3.

Article 12 – Sanctions for non-compliance

Non-compliance **12.1** Non-compliance of Oracle employees with this Processor Code may result in disciplinary action in accordance with Oracle policies and local law, up to and including termination of employment.

Article 13 – Conflicts between this Processor Code and Applicable Processor Law

Conflict between Processor Code and law **13.1** Where there is a conflict between Applicable Processor Law and this Processor Code, the relevant Responsible Line of Business Executive shall consult with the Privacy Office to determine how to comply with this Processor Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal requirements **13.2** The relevant Responsible Line of Business Executive, in consultation with the legal department, shall promptly inform the Privacy Office of any new legal requirement that may interfere with Oracle's ability to comply with this Processor Code.

Reporting to Lead SA and Customer SA **13.3** If Oracle becomes aware that Applicable Processor Law or any change in Applicable Processor Law is likely to have a substantial adverse effect on Oracle's ability to meet its obligations under 3.1, 3.2 or 10.3, Oracle will report this to the Lead SA and the Customer SA.

Article 14 – Changes to this Processor Code

Approval for Changes **14.1** Any changes to this Processor Code require the prior approval of the General Counsel and shall thereafter be communicated to the Group Companies.

Effective Date Of Changes

14.2 Any amendment shall enter into force after it has been approved and made available to Customers on the Oracle Internet site (www.oracle.com).

Prior Versions

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

Notification to Lead SA and Customers

14.4 The Global Data Protection Officer shall be responsible for informing the Lead SA of material changes to this Processor Code, if any, on a yearly basis, including a brief explanation of the reasons justifying the update. Where a change to this Processor Code has a significant impact on the Processing conditions of Personal Information, 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.

Article 15 – Transition Periods

Transition Period for New Group Companies

15.1 Except as otherwise indicated, any entity that becomes a Group Company after the Effective Date shall comply with this Processor Code upon becoming a Group Company.

Transition Period for Divested Entities

15.2 A Divested Entity will remain covered by this Processor Code after its divestment for such period as is required by Oracle to disentangle the Processing of Personal Information relating to such Divested Entity.

Transition Period for IT Systems

15.3 Where implementation of this Processor Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be up to two years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition Period for Existing Agreements

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

ANNEX 1: Definitions

Affected Individual	AFFECTED INDIVIDUAL shall mean the individual referred to in Article 11.1
Applicable Controller Law	APPLICABLE CONTROLLER LAW shall mean the Data Protection Laws of the EEA Countries that are applicable to the Customer as the Controller of Personal Information.
Applicable Processor Law	APPLICABLE PROCESSOR LAW shall mean the Data Protection Laws that are applicable to Oracle as the Processor of Personal Information.
Global Data Protection Officer	GLOBAL DATA PROTECTION OFFICER shall mean the officer referred to in Article 8.1
Controller	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.
Customer	CUSTOMER shall mean the customer who has entered into a contract with Oracle for the delivery of Oracle Services.
Customer SA	CUSTOMER SA shall have the meaning set forth in Article 10.3.
Customer Individual	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.
Customer Personal Information	CUSTOMER PERSONAL INFORMATION shall mean Personal Information of a Customer Individual.
Data Protection Law	DATA PROTECTION LAW shall mean the laws of a 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.

Divested Entity	DIVESTED ENTITY shall mean the divestment by Oracle of a Group Company or business by means of: (i) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or (ii) a demerger, sale of assets, or any other manner or form.
EEA Countries	EEA COUNTRIES (European Economic Area Countries) shall mean all Member States of the European Union, Norway, and for purposes of this Processor Code, Switzerland and the UK post-Brexit.
EEA Data Protection Law	EEA DATA PROTECTION LAW shall mean the data protection laws of the EEA Countries, Switzerland, and (post-Brexit) the United Kingdom.
EEA Data Transfer Restriction	EEA DATA TRANSFER RESTRICTION shall mean any restriction under EEA Data Protection Law regarding outbound transfers of Personal Information.
Effective Date	EFFECTIVE DATE shall mean the date on which this Processor Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean an employee of Oracle.
General Counsel	GENERAL COUNSEL shall mean the General Counsel of Oracle Corporation.
Group Company	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.
Lead SASA	LEAD SASA shall mean the supervisory authority of Ireland.

Mandatory Requirements	MANDATORY REQUIREMENTS shall mean mandatory requirements of Applicable Processor Law which do not go beyond what is necessary in a democratic society i.e. which constitute a necessary measure to safeguard national security defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the state or the protection of a Customer Individual or the rights and freedoms of others.
Oracle	ORACLE shall mean Oracle Corporation and its Group Companies.
Oracle Contracting Entity	ORACLE CONTRACTING ENTITY shall mean the Oracle Group Company that has entered into a Services Contract for the provision of Services.
Oracle Corporation	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	ORACLE EMEA shall mean Oracle EMEA Limited, having its registered seat in Dublin, Ireland.
Oracle Sub-processor	ORACLE SUB-PROCESSOR shall mean any Group Company engaged by Oracle as a Sub-processor.
Personal Information	PERSONAL INFORMATION shall mean any information relating to an identified or identifiable individual.
Privacy Professional	PRIVACY PROFESSIONAL shall mean the privacy professionals appointed by the Global Data Protection Officer pursuant to Article 8.3.
Processing	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.
Processor	PROCESSOR shall mean the entity or natural person which Processes Personal Information on behalf of a Third Party Controller.

Processor Code	PROCESSOR CODE shall mean this f for Processing Personal Information of Customer Individuals.
SA	SA shall mean any supervisory authority of one of the EEA Countries.
Responsible Line of Business Executive	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.
Services	SERVICES shall mean the services listed in Article 4.1 as contracted by the Customer under the Services Contract.
Services Contract	SERVICES CONTRACT shall mean the contract for delivery of Services entered into between an Oracle Group Company and the Customer pursuant to Article 2.1.
Staff	STAFF shall mean all Employees and other persons who Process Personal Information as part of their respective duties or responsibilities, either using Oracle information technology systems or working primarily from Oracle premises.
Sub-processor	SUB-PROCESSOR shall mean any Processor engaged to Process Personal Information as a sub-processor.
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or government authority) outside Oracle or a Customer.
Third Party Sub-processor	THIRD PARTY SUB-PROCESSOR shall mean any Third Party engaged by Oracle as a Sub-processor.
Third Party Sub-processor Contract	THIRD PARTY SUB-PROCESSING CONTRACT shall mean the validly entered into written or electronic agreement between Oracle and the Third party Sub-processor pursuant to Article 7.2.
Interpretations	INTERPRETATION OF THIS PROCESSOR CODE:

(i) Unless the context requires otherwise, all references to a particular Arti- cle or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in con- struing any provision of this Processor Code

(iii) if a word or phrase is defined, its other grammatical forms have a corre- sponding meaning

(iv) the male form shall include the female form

(v) 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

(vi) a reference to a document (including, without limitation, a reference to this Processor Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Processor Code or that other document, and

(vii) a reference to law includes any regulatory requirement, sectorial recom- mendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2: Oracle Corporate Security Practices

Introduction

The Oracle Corporate Security Practices ("Security Practices") describe the security practices implemented pursuant to Oracle's Corporate security program, and adhered to by Oracle for its operational and services infrastructure under its control, including Oracle's corporate network and systems. As used 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 customer's Oracle Cloud instance. Third parties engaged by Oracle and that are also provided access to customer data by Oracle ("subprocessors"), will be contractually committed to materially equivalent security practices.

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.

1. Scope

1.1 Overview

The Security Practices are designed to protect the confidentiality, integrity, and availability of both customer and Oracle data. Oracle continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers.

As noted above, this document describes the security practices adhered to by Oracle for its operation and services infrastructure. Companies that Oracle acquires are required to align with these Security Practices as part of the integration process.

Oracle's Consulting and Advanced Customer Support Services lines of business have also developed more detailed statements of security practices that apply to many of their service offerings, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Global Customer Support Security Practices Consulting Security Practices
- Advanced Customer Services Security Practices

2. Oracle Information Security

2.1 Overview

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 Employees, contingent workers, and sub-processors. They are generally aligned with the ISO/IEC 27002:2013 and 27001:2013 standards, and govern all areas of security within Oracle.

Oracle takes a holistic approach to information security, implementing a multilayered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

2.2 Privacy

The *Oracle Privacy Policy* describes how Oracle collects and uses personal information collected from the Oracle websites that link or refer to the policy as well as from offline sales and marketing activities. It also describes how users can control that collection and use. This policy is available at https://www.oracle.com/legal/privacy/privacy-policy.html.

The *Oracle Services Privacy Policy* describes Oracle's treatment of data that resides on Oracle, customer or third-party systems (including personal information or "PI") to which Oracle may be provided access in connection with the provision of services. This policy is available at https://www.oracle.com/legal/privacy/services-privacy-policy.html.

The *Oracle Marketing Cloud and Oracle Data Cloud Privacy Policy* describes how Oracle Marketing Cloud and Oracle Data Cloud services facilitate the collection and use of information by our customers in connection with interest-based advertising, and is designed to provide tools to help understand and control the collection and use of that information. This policy is available at https://www.oracle.com/legal/privacy/marketing-cloud-data- cloud-privacy-policy.html.

2.3 Enforcement

Oracle requires the reporting of and response to information security incidents in a timely and efficient manner. Oracle also maintains a detailed Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

Oracle's Global Information Security (GIS) organization conducts security reviews, assessments, and audits periodically to confirm compliance with the Oracle information security policies, procedures, and practices.

Where non-compliance is found, GIS works with the relevant Lines of Business to resolve those issues in a timely a manner. GIS reserves the right to intervene as deemed necessary and to isolate environments in non-compliance that put infrastructure or other environments at serious risk.

Oracle employees who fail to comply with Oracle information security policies, procedures, and practices may be subject to disciplinary action, up to and including termination.

3. 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, who reports directly to the CTO, manages the functional departments directly responsible for identifying and implementing security controls at Oracle. The Global Information Security, Global Product Security, Global Physical Security, and Oracle Security Architecture organizations comprise Oracle Corporate Security, which provides independent security policy, guidance and compliance oversight to Oracle worldwide.

3.1 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.

3.2 Global Security Organizations

3.2.1 Global Information Security

Global Information Security (GIS) is responsible for security oversight and assurance, policy compliance and enforcement, leading the development of information security policy and strategy, as well as training and awareness at the Corporate level. GIS serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.

3.2.2 Global Product Security

Global Product Security (GPS) acts as a central resource to help Oracle development teams improve the security of Oracle products. GPS' primary mission is to promote the use of the Oracle Software Security Assurance (OSSA) standards throughout Oracle. Responsibilities include assisting in improving the security of Oracle products in their development phase, performing security assessments of Oracle products using a variety of techniques, and evaluating potential product security vulnerabilities.

3.2.3 Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of our employees, business enterprise and assets. More information on applicable physical security controls are described in section 6.

3.2.4 Corporate Security Architecture

Corporate Security Architecture (CSA) is responsible for setting Information Security Architecture strategy and direction in support of long-term Corporate objectives and verifying alignment of IT initiatives with Corporate Security Architecture strategy and direction. In addition, CSA identifies and guides IT security infrastructure improvements and reviews security-related technical aspects of IT projects and acts as technical advisor on Corporate Security matters.

3.3 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.

3.4 Confidentiality Agreements

All Oracle employees and subprocessors who may have access to customer data are subject to a written confidentiality agreement. Prior to performing services for Oracle and prior to accessing any Oracle system or resource, service providers are required to sign a Services Provider Agreement, a Network Access Agreement, and a work order defining the services to be provided.

Oracle is obligated to protect the confidentiality of customer data in accordance with the terms of the Ordering Document, Exhibit, and Statement of Work.

3.5 Independent Review of Information Security

Global Information Security, in conjunction with Oracle Internal Audit, oversees compliance of the security controls, processes, and procedures for Oracle services.

4. Asset Classification and Control

4.1 Responsibility, Inventory, and Ownership of Assets

Overarching controls related to assets are addressed by the *Oracle Information Protection Policy*, the *Oracle Desktop and Laptop Security Policy*, the *Oracle Information Systems Inventory Policy,* and the *Oracle Acceptable Use Policy for Company Resources*. All information assets have an owner who is responsible for the protection and inventory of assets based on the sensitivity and value of information. If ownership has not been assigned, it will default to the administrators of the application or system. This includes maintenance of operations guides and other documentation describing the environments.

4.2 Asset Classification and Control

Oracle provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications in order to provide protection for Oracle and customer information assets. Oracle has defined three classes of confidential information – Internal, Restricted, and Highly Restricted – with each classification requiring corresponding levels of security controls (e.g., encryption requirements for data classified as Restricted or Highly Restricted). Customer data is classified as among Oracle's top two categories of confidential information, which have associated limits on access, distribution and handling. Oracle keeps the information confidential in accordance with the terms of customer's order.

5. Human Resources Security

Oracle places a strong emphasis on personnel security. Measures taken to minimize risks associated with human error, theft, fraud, and misuse of facilities include personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

The *Oracle Code of Ethics and Business Conduct* sets forth Oracle's high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business throughout the world. The standard applies to Oracle employees, contractors, and temporary employees. It covers the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required every two years. The Code of Ethics and Business Conduct is available at the following URL: http://www.oracle.com/us/corporate/investor- relations/cebc-176732.pdf

5.1 Employee Screening

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 Oracle policy.

5.2 Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters, ad hoc security awareness campaigns, and security related Corporate send mails.

Each employee is required to complete information protection awareness training. The course instructs employees on their obligations under the various Oracle privacy and security policies (such as the *Information Protection Policy*, *Acceptable Use Policy for Company Resources* and the *Services Privacy Policy*). The course also covers data privacy principles and data handling practices that may apply to employees' jobs at Oracle and are required by company policy, including those related to use, access, integrity, sharing, retention, security and disposal of data.

Oracle performs periodic compliance reviews to determine if employees have completed the online awareness-training course. If Oracle determines that an employee has not completed the required course, the employee will be promptly notified and instructed to complete the required training, and may be subject to disciplinary action.

Oracle promotes awareness of, and educates employees about, issues relating to security. Oracle currently prepares and distributes to its employees quarterly newsletters, ad hoc notices and other written material on security. Oracle also may update existing training courses, and develop new courses from time to time, which employees will be directed to complete.

5.3 Enforcement

Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information security policies, procedures, and practices. Employees who fail to comply with Oracle information security policies, procedures and guidelines may be subject to disciplinary action, up to and including termination.

6. Physical Security

Overarching controls related to physical security are described in the *Oracle Identification and Access Badge Policy*. Oracle Global Physical Security utilize a security risk-based defense in depth or layered methodology designed to balance prevention, detection, protection and response.

Oracle maintains the following physical security standards designed to prohibit unau thorized physical access at all Oracle facilities from which customer data may be handled ("Service Locations"):

- Service Locations have physical access limited to Oracle employees, subcontractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on the premises.
- Visitors to Service Locations are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement.
- Security monitors the possession of keys/access cards and the ability to access the Service Locations. Staff leaving Oracle employment must return keys/cards.

After-hours access to Service Locations is monitored and controlled by Security.

Oracle Physical Security authorizes all repairs and modifications to the security barriers and entry controls at Service Locations owned by Oracle.

7. Communications and Operations Management

Oracle aligns with the IT service management process areas as outlined in the ITIL Infrastructure Library and uses this framework as a guide for operational delivery. Oracle's internal documentation specifies current operational processes and procedures for employees' performance of technical functions.

7.1 Segregation of Duties

Roles within operations are well defined, allowing for segregation of duties. Segregation of duties is achieved by organizing operations into functional groups, where each function is performed by separate groups of employees. Examples of the functional groups include database administrators, System Administrators, and network engineers.

7.2 Protection Against Malicious Code

Oracle's Desktop and Laptop Security Policy requires that all computers connected to Oracle's intranet have anti-virus, firewall and desktop asset management software installed, that all computers that hold Oracle data running a Windows operating system must have Microsoft security updates enabled, and that Oracle personnel install the approved full disk encryption software on their laptops, unless an approved exception has been authorized for appropriate business purposes.

Oracle's Global IT (GIT) organization keeps anti-virus products up-to-date with virus definitions and security updates. GIT is responsible for notifying internal Oracle system users of any credible virus threats and when security updates are available and Oracle employees are required to comply with instructions received through e-mail from the GIT organization. Oracle has also licensed and installed third-party anti-virus and anti-spam products to scan all emails and attachments (inbound and outbound).

7.3 Network Security Management

Overarching policies related to network infrastructure are described in the *Oracle Network Security Policy* and *Oracle Server Security Policy*. Oracle employs intrusion prevention and detection systems within the Oracle corporate networks to provide surveillance for intercepting and responding to security events as they are identified. Events are analyzed using signature and anomaly detection and Oracle updates the signature database frequently. Alerts are forwarded to Oracle's IT security for review and response to potential threats. Oracle uses router rules, access control and security lists and segmentation on the Oracle network. Oracle's Global IT and Cloud DevOps departments manage and monitor routers and firewall logs and network devices are safeguarded via centralized authentication with audited usage.

7.4 Monitoring and Protection of Audit Log Information

The following sections describe controls utilized by Oracle to monitor and protect audit log information as detailed in the overarching *Oracle Logging and Log Analysis Policy.*

Logging

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 to protect against operational issues, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.

Log Review

Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security incident management process.

Log Security

Access to logs is provided on the basis of need to know and least privilege. Where feasible, log files are protected by cryptographic hash sum, and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet-accessible.

8. Access Control

Overarching policies for access are described in the *Oracle Logical Access Controls Policy*. Access control refers to the policies, procedures, and tools that govern the access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol.

Oracle uses the principle of "Least privilege" 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.

Oracle uses the principle of "Default deny" that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.

In the event of employee terminations, deaths or resignations, Oracle will take actions to terminate network, telephony and physical access for such former employees. Oracle Corporate Security will periodically review accounts of terminated employees to verify that access has been terminated and that stale accounts are removed from the Oracle network

8.1 Access Control

The *Oracle 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. The policy does not apply to publicly accessible internet-facing Oracle systems or customer's end users.

8.2 User Access Management

User Registration

- Access privileges are granted based on job role and require management approval.

Privilege Management

- Authorization is dependent on 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" - Only provide access when required for job function or role
- "Segregation of duties" - Avoid a conflict of interest in the access that is provided
- "Least privilege" - Restricted access to only those resources and information required for a legitimate busi- ness purpose

User Password Management

As described in the *Oracle Password Policy*, Oracle enforces strong password policies for Oracle network, operating system, and database accounts in an effort to reduce the chances of intruders gaining access to systems or environments through exploitation of User accounts and their associated passwords.

Review of Access Rights

Network and operating system accounts are reviewed regularly with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to terminate network, telephony, and physical access for such former employees.

Password Use

The use of passwords is addressed in the *Oracle Password Policy.* Oracle employees are obligated to follow rules for password length and complexity, and keep their passwords confidential and secure at all times. Passwords may not be disclosed to any unauthorized person. Under certain circumstances, passwords may be communicated between authorized Oracle employees for the purpose of providing support services.

8.3 Network Access Controls

Network controls implemented for Oracle address the protection and control of customer data during its transmission from one end system to another. The *Oracle Use of Network Services Policy* states that computers, servers, and other data devices connected to the Oracle network must comply with Global IT (GIT) and GIS standards for security, configuration, and access method, in accordance with *Oracle's Acceptable Use Policy for Company Resources.*

9. Information Systems Acquisition, Development, and Maintenance

9.1 Access Control to Program Source Code

Access to Oracle source code is provided on a strict "Need to know" basis to those who require it for an authorized business purpose.

9.2 Technical Vulnerability Management

Oracle subscribes to vulnerability notification systems to stay apprised of security Incidents, advisories, and other related information. Oracle takes actions on the notification of a threat or risk once it has the opportunity to confirm that both a valid risk exists and that the recommended changes are applicable to the particular system or environment.

10. Information Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to, or handling of, customer data in its possession or under its control, whether the data is held on Oracle hardware assets, those of vendors/suppliers, or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Global Information Security (GIS) organization is required to be informed of such incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those incidents.

If Oracle becomes aware and determines that an incident involving your customer data qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data transmitted, stored or otherwise processed on Oracle systems that compromises the security, confidentiality or integrity of such customer data, Oracle will report such breach to you without undue delay.

Oracle will not disclose production data located on Oracle systems, including text and images, except in accordance with your order, your instructions, or to the extent required by law. Oracle will use diligent efforts to inform you, to the extent permitted by law, of any request for such disclosure before disclosure is made.

11. Oracle's Resilience Management

Oracle has a global Risk Management and Resiliency Program (RMRP), which comprises, among other elements, contingency planning and plan testing designed to enable our critical, internal operations to continue in spite of potentially business-disruptive incidents. The RMRP addresses:

- Personal safety;
- Incident management;
- Business continuity; and
- Technological system recovery.

12. Audit

In the event that the applicable order for services provides you with the right to audit Oracle's compliance with these security practices, the following procedures apply. You must send Oracle's Global Information Security organization a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. The parties will work cooperatively to agree on a final audit plan. The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to on-site policies and regulations, and may not unreasonably interfere with business activities. If you would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle. Upon completion of the audit, you will provide Oracle with a copy of the audit report, which is classified as confidential information under the terms of the Agreement. Additional audit terms may be included in your order for services.

13. Customer Data Retention

Except as otherwise specified in an order for services or required by law, upon termination of services or at your request, Oracle will delete your production customer data located on Oracle computers in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the data. For Cloud Services, customer data management is generally "self service" and additional information on features to assist you with data management can be found in the applicable "Service Feature Guidance" document. For other Oracle services, you may consult with your Oracle services contact for additional information on data deletion prior to service completion.

As described in the *Oracle Media Sanitization and Disposal Policy*, media containing Customer Data will be securely sanitized, or destroyed and disposed of when the media is no longer required or able to be used, or the storage media becomes otherwise obsolete. Currently approved sanitization methods are degaussing, shredding, incineration, and verified overwrites of the data. Some hardware such as SSD may include acceptable built-in secure erasure functionality.

14. Reference

As stated above, these security practices should be read in conjunction with any more detailed security practices created by Oracle's Cloud Consulting and Advanced Customer Services lines of business, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Global Customer Support Security Practices Consulting Security Practices
- Advanced Customer Services Security Practices

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.

APPENDIX 5 TO ORACLE PRODUCT TERMS

TUPE

1. DEFINITIONS CLAUSE

The following definitions will apply in this Appendix:

"**Buyer Personnel**" means the Buyer's employees and any other person who prior to the commencement of any Services under this Agreement provides the Services or services similar to the Services for the Buyer;

"**Contracts Act**" means the Contracts (Rights of Third Parties) Act 1999 as amended or replaced from time to time;

"**Employment Law**" means all and any laws, including, without limitation, directives, statutes, secondary legislation, orders, codes of practice, contractual obligations and common law, whether of the European Union, any member of the European Union, or any other country where this agreement applies or other relevant authority, relating to or connected with, whether on an individual or collective basis: (1) the employment and dismissal of employees (including their health and safety at work, and information and consultation and collective bargaining); and (2) the engagement, use and termination of individuals other than employees who provide services (including their health and safety at work);

"**Employment Liabilities**" means all actions, proceedings, losses, damages, liabilities, compensation, awards, fines, penalties, costs (including legal costs), demands, orders, expenses or other payments connected with or arising from Employment Law;

"**Supplier Personnel"** means the Supplier's employees and any other person who provides the Services on behalf of the Supplier;

"**Regulations**" means the law implementing in any jurisdiction the European Council Directive 2001/23/EEC on the approximation of laws of European member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or replaced from time to time, and any other legislation which has the same or similar effect;

"**Replacement Services**" means all or part of the Services or services substantially similar to all or part of the Services which are provided by an entity other than the Supplier following the termination of the provision of the Services (whether in whole or in part) under this Agreement;

"**Successor Supplier**" means any entity (including the Buyer) which provides the Replacement Services;

2. EMPLOYMENT PROVISIONS - COMMENCEMENT OF SERVICES

2.1. The Supplier and the Buyer do not intend that any Buyer Personnel will become employees of the Supplier or any sub-contractor upon the commencement of any Services under this Agreement pursuant to the Regulations.

2.2. If it is found or alleged that the employment of any person transfers to the Supplier or its sub-contractor at commencement of the Services under this Agreement pursuant to the Regulations:

2.2.1. the Supplier shall notify the Buyer (or shall procure that its sub-contractor shall notify the Buyer) and the Buyer shall notify the Supplier (and any relevant sub-contractor)

of that finding or allegation as soon as reasonably practicable after becoming aware of it;

2.2.2. the Buyer may within seven (7) days after becoming aware of that allegation or finding referred to in Clause 2.2.1 offer to employ or engage that person on such terms as the Buyer shall determine and the Supplier shall (and shall procure that its sub-contractor shall) give all reasonable assistance requested by the Buyer to persuade that person to accept the offer; and

2.2.3. within twenty-eight (28) days after becoming aware of the allegation or finding referred to in Clause 2.2.1 the Supplier (or any relevant sub-contractor) may dismiss that person and Buyer shall indemnify and keep indemnified the Supplier and its sub-contractor against all Employment Liabilities which the Supplier and/or its sub-contractor may suffer or incur in relation to that dismissal and the employment of that person up to the date of that dismissal in each case **PROVIDED** that the Supplier or its sub-contractor takes all reasonable steps to minimise those Employment Liabilities and save for any Employment Liabilities which arise in respect of a finding that the Supplier or its sub-contractor unlawfully discriminated against that person.

2.3. The Buyer will indemnify and keep indemnified the Supplier (and any relevant sub-contractor) against any and all Employment Liabilities arising out of or in connection with any claim or demand by any Buyer Personnel or Representative arising out of or in connection with:

2.3.1. the employment or engagement of any Buyer Personnel by the Buyer or a third party (including the termination of such employment or engagement) prior to the commencement of the Services under this Agreement; or

2.3.2. the transfer or alleged transfer of the employment of the Buyer Personnel to the Supplier (or any relevant sub-contractor) pursuant to the Regulations including for the avoidance of doubt liability arising from a failure to comply with any information or consultation requirements under the Regulations.

3. TERMINATION OF SERVICES

3.1. Neither the Supplier nor the Buyer intend that any Supplier Personnel will become employees of the Buyer or a Successor Supplier pursuant to the Regulations upon termination of the Services (whether in whole or in part).

3.2. If it is found or alleged that the employment of any of Supplier Personnel transfers to the Buyer or a Successor Supplier upon termination of this Agreement pursuant to the Regulations:

3.2.1. the Supplier shall notify the Buyer (or shall procure that its sub-contractor shall notify the Buyer) and the Buyer shall notify the Supplier (and any relevant sub-contractor) of that finding or allegation as soon as reasonably practicable after becoming aware of it;

3.2.2. the Supplier or any relevant sub-contractor may within seven (7) days after becoming aware of that allegation or finding referred to in Clause 3.2 offer to employ or engage that person on such terms as the Supplier or the relevant sub-contractors shall determine and the Buyer shall (and shall procure that the Successor Supplier shall) give all reasonable assistance requested by the Supplier or the relevant sub-contractor to persuade that person to accept the offer; and

3.2.3. within twenty-eight (28) days after becoming aware of that allegation or finding referred to in Clause 3.2, the Buyer or the Successor Supplier may dismiss that person and the Supplier shall indemnify and keep indemnified the Buyer and any Successor Supplier against all Employment Liabilities which the Buyer or the Successor Supplier may suffer or incur in relation to that dismissal and the employment of that person up to the date of that dismissal in each case PROVIDED the Buyer (or the Successor Supplier, as applicable) takes all reasonable steps to

minimise those Employment Liabilities and save for any Employment Liabilities which arise in respect of a finding that the Buyer (or the Successor Supplier, as applicable) unlawfully discriminated against that person.

3.3. The Supplier will indemnify and keep indemnified the Buyer and any Successor Supplier against any and all Employment Liabilities arising out of or in connection with any claim or demand by any Supplier Personnel or Representative arising out of or in connection with:

3.3.1. the employment or engagement of any Supplier Personnel by the Supplier or a third party sub-contractor (including the termination of such employment or engagement) prior to the transfer date or alleged transfer date pursuant to the Regulations; or

3.3.2. the transfer or alleged transfer of the employment of the Supplier Personnel to the Buyer or a Successor Supplier pursuant to the Regulations including for the avoidance of doubt liability arising from a failure to comply with any information or consultation requirements under the Regulations.

4. THIRD PARTY RIGHTS

For the purposes of the Contracts Act it is intended that the Successor Supplier and any relevant sub-contractor of the Supplier will have the right to enforce any rights conferred on them by Clauses 2.2, 2.3, 3.2 and 3.3 and to that extent the Successor Supplier or any relevant sub-contractor of the Supplier will have the same rights against the Buyer or the Supplier (as relevant) as would be available if the Successor Supplier or any relevant sub-contractor of the Supplier were parties to this Agreement. Save as expressly provided under this section 4, no third party will have the right to enforce any term of this Agreement, and the Contracts Act will not apply. Notwithstanding the rights conferred by this section 4, the parties may by agreement, rescind this Agreement or vary it in any way without the consent of the Successor Supplier or any relevant sub-contractor of the Supplier.

APPENDIX 6 TO ORACLE PRODUCT TERMS

ADDITIONAL LICENSES AND ORACLE LINUX SUPPORT

You have ordered Oracle Cloud Services under the Call-Off Contract and have obtained additional licenses and support in connection with the Oracle Cloud Services, where such licenses and support are not provided by Oracle under the terms of Framework Agreement RM6292. Oracle has therefore agreed that, for all Oracle Cloud Services purchased under the Call Off Contract You will receive during the term of the Call-Off Contract:

- Oracle Linux Premier Support that will be provided in accordance with the Oracle Linux and Oracle VM Support Policies (http://www.oracle.com/us/support/library/enterprise-linux-support-policies-069172.pdf).
- a free license for each of the products listed on the following web page: https://oss.oracle.com/licenses/oci-included-apps/index.html, in each case under the terms linked for each product on that page. Oracle does not provide technical support for any of the products listed there.
- a free Oracle Java SE license for Your instances in the Oracle Public Cloud that will be provided in accordance with the Oracle Technology Network License Agreement for Oracle Java SE found here: https://java.com/otnlicense. You will also receive Oracle Cloud Support for Oracle Java SE for the foregoing usage and that technical support will be provided in accordance with the Oracle Hosting and Delivery Policies available at https://oracle.com/contracts.
- a free Oracle GraalVM Enterprise Edition license for Your instances in the Oracle Public Cloud that will be provided in accordance with the Oracle Technology Network License Agreement for GraalVM Enterprise Edition found here: https://www.oracle.com/technetwork/licenses/graalvm-otn-license-5486575.html. You will also receive Oracle Cloud Support for Oracle GraalVM Enterprise Edition for the foregoing usage and that technical support will be provided in accordance with the Oracle Cloud Hosting and Delivery Policies available at https://oracle.com/contracts.

You acknowledge that although the above licenses and support will be provided in connection with the Oracle Cloud Services, they do not fall within the scope of the Call-Off Contract and are not subject to the terms and conditions of the Call-Off Contract or Framework Agreement RM6292. You therefore accept that Your use of such licenses and support shall be governed by the above terms notwithstanding anything to the contrary in the Call-Off Contract or Framework Agreement RM6292.