Crown Commercial Service

RM6111 Cloud Compute
Framework Schedule 4 Annex 1

Order Form

1. This Order Form is issued in accordance with the provisions of the Cloud Compute Framework Agreement RM6111 dated *05/04/2021* 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 Call-Off Terms. The Call-Off Terms are substantially 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*, the agreed Call-Off Terms for the Contract being those set out in Annex 1 to this Order Form.

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 Call-Off Terms.

5. This Order Form shall comprise:

   (a) This document headed "Order Form";
   (b) Attachment 1 – Service Descriptions and Product Terms;
   (c) Attachment 2 – Service Level Agreement(s);
   (d) Attachment 3 – Charges and Payment Profile;
   (e) Attachment 4 – Schedule of Standards;
   (f) Attachment 5 – Schedule of Processing, Personal Data and Data Subjects;
   (g) Attachment 6 – Alternative Clauses;
   (h) Attachment 7 – Supplier's Acceptable Use Policy;
   (i) Attachment 8 – Data Processing Agreement (which shall include the Protective Measures (as defined in the Call-Off Terms));
   (j) Annex 1 – Call-Off Terms; and
   (k) Annex 2 – Applicability Matrix.

6. The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

   (a) subject always to Clauses 2.5 and 4.2.2 of the Call-Off Terms, the Special Terms (if any);
   (b) this Order Form (except any Applicable Supplier Terms or Special Terms (as defined in the Call-Off Terms));
   (c) the Call-Off Terms (as set out in Annex 1 to this Order Form);
   (d) the Applicable Supplier Terms;
   (e) the applicable provisions of the Framework Agreement, except (and subject always to Clause 2.4 of the Call-Off Terms) Schedule 13 (Tender) of the Framework Agreement; and
   (f) Schedule 13 (Tender) of the Framework Agreement.

7. As an aid to interpretation of the Contract, the Applicability Matrix set out in Annex 2 (Applicability Matrix) to this Order Form identifies:

   (a) each of the relevant documents which contain contractual provisions that apply to the Contract; and

   (b) in respect of each such document the particular contractual provisions in that document which apply to the Contract.

8. 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.

9. 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.

10. 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:	DWP_Oracle_OCI Hosting
Contract Title:	Oracle Cloud Infrastructure (OCI) Hosting for Pensions Transformation Programme Customer Account Manager (PTP CAM Suite) Proof of Concept (POC)
Contract Description:	Oracle Platform as a Service (PaaS) Cloud Services and for Oracle Infrastructure as a Service (IaaS) Cloud Services for the Buyer POC for a path to go-live for OCI Hosting of the PTP CAM Suite. A consumption-based hosting service (Buyer internal description: development and testing hosting environments known internally as the "**PTP CAM Project**").
Commencement Date:	The Commencement Date for each Service will be the date that the Buyer are issued access that enables the Buyer to activate Buyer's Services

Buyer details	
Buyer organisation name: Department for Work and Pensions (DWP)	
Billing address: Your organisation's billing address - please ensure you include a postcode. Brunel Way, Blackpool Fylde Industrial Estate, Blackpool & Fylde Industrial Estate, GB, FY4 5DR	
Buyer Authorised Representative name: The name of the person authorised to manage this Contract for the Buyer. REDACTED FOI 40	
Buyer Authorised Representative contact details: Email and telephone contact details for the Buyer's representative Email: REDACTED FOI 40 Phone REDACTED FOI 40	

Crown Commercial Service

Buyer User details:

Those employees, contractors, and end users, as applicable, authorised by the Buyer or on the Buyer's behalf to use the Services in accordance with this Supplier Product Terms and this Order Form. For Services that are specifically designed to allow the Buyer's clients, agents, customers, suppliers or other third parties to access the Services to interact with the Buyer, such third parties will be considered "Users".

Expanded Usage Rights

REDACTED IN FULL

Crown Commercial Service

Supplier details

Supplier name:
The Supplier's legal entity name, as it appears in the Framework Agreement.

Oracle Corporation UK Limited

Supplier address:
Supplier's registered office address.

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

Supplier authorised representative name:
The name of the person authorised to manage this Contract for the Supplier.

REDACTED FOI 40

Supplier authorised representative contact details:
Email and telephone contact details of the Supplier' authorised representative.

Email: REDACTED FOI 40

Telephone: REDACTED FOI 40

Order reference number:
A unique number provided by the Supplier at the time of quote.

REDACTED FOI 43

Key Sub-Contractors and Sub-processors:	The Supplier's Key Sub-Contractors are currently REDACTED FOI 40 and REDACTED FOI 40 and Sub- processors are as set out in the Supplier's Register of Key Sub-Contractors and Sub-processors which is available at: Subject always to Clause 15.12 of the Call-Off Terms, the Supplier is obliged to maintain the Register of Key Sub-Contractors and 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 Key Sub-Contractors and 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:

12 months from the Commencement date.

Extension Period:

No extension to the term above.

Special Security or compliance requirements:

Include any security, conformance or compliance requirements with which the Services must comply with.

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 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 Call-Off Terms:

1. **Government Discount(s)**

   Not Applicable

2. **Hyperlinks within Service Descriptions and Applicable Supplier Terms**

The references in this Order Form and applicable Attachments to the following documents contain words, phrases or specific web addresses that allows the Buyer to click through to another section of the same document or to a URL which contains a policy, terms and conditions or any other document ("**Additional Hyperlinks**").

- **OCI Services Descriptions – Attachment 1: 249 pages (effective date 10 June 22 no version number**
- **Oracle Cloud Hosting and Delivery Policies – Attachment 2 V3.3 18 pages**
- **Oracle PaaS and IaaS Public Cloud Services Pillar document – Attachment 2 December 22 108 pages**
- **Oracle Data Protection Agreement – Attachment 8 v01012023 9 pages**

To the extent only the then-current Additional Hyperlinks that apply to the Services provided under this Order Form, such Additional Hyperlinks are incorporated by reference to this Order Form and deemed effective. Where the Supplier has used Additional Hyperlinks in this Order Form to supplement the Supplier Service Descriptions and Applicable Supplier Terms, the Supplier, during the Term of the Contract, shall not materially reduce the level of performance, security, or availability of the Services under this Order Form.

The Buyer may subscribe to receive an alert about updates to Oracle Cloud Hosting and Hosting and Delivery Policies and Services Descriptions (and other Services Descriptions made available by Oracle) at REDACTED FOI 40

Crown Commercial Service

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.

Services required:	The Services to be provided by the Supplier: please see Attachment 1 (Service Descriptions and Product Terms) for those Services which are potentially in scope. The Buyer still has to go through the Service Request process (below) to crystallise the exact purchase.
Service Request process (dynamic nature of Services):	The Buyer can provision and manage your Oracle Cloud services as follows: Oracle Cloud Infrastructure Console (otherwise known as the Supplier Portal). The Console is an intuitive, graphical interface that lets you create and manage your instances, cloud networks, and storage volumes, as well as your users and permissions. To access the Console, you must use a supported browser (Google Chrome 69 or later, Safari 12.1 or later, Firefox 62 or later) Instructions on how to access and use the Oracle Cloud Infrastructure Console are set out in Oracle's Cloud Infrastructure Getting Started Guide which is available here: REDACTED FOI 40 The Buyer is responsible for ensuring that any account identification details (or similar account administration information) are reported to the Supplier to assist the Supplier in administering the provision of Services under this Contract.
Geographical limitations on the location(s) from which the Services will be provided:	It is acknowledged that: (a) the Buyer is responsible for selecting the country and/or more specific geographic region(s) from which the Services are to be provided and/or within which it permits the Supplier to process Buyer Content (including Personal Data); and (b) the Supplier is responsible for ensuring that the Services are only provided and/or Buyer Content is only located within the country(ries) and/or more specific geographic region(s) instructed by the Buyer from time to time in accordance with this Contract, except as noted in (c) below. (c) The following exceptions to the location of Services and any other circumstances that may cause Personal Data to move to a Restricted Country in a manner that is outside of the Buyer's control were submitted by the Supplier in their tender. If the Buyer reasonably expects to make use of these Services or that the Buyer would find itself in such circumstances, then the Buyer should tick the Restricted Country box below and the Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Alternatively, the Buyer may elect not to use the relevant services. In the course of the provision of the Services, Buyer Content may be accessed by Oracle personnel from various locations worldwide as described in the

	relevant Service Descriptions strictly as necessary in order to provide the Services. Where this occurs any such access will be governed by Oracle's adopted Binding Corporate Rules in order to ensure an adequate level of protection as required by applicable as required by data protection legislation. As at the Commencement Date the Buyer instructs the Supplier that the Services are only delivered from data centres sited in the countries and/or more specific geographical regions listed below. **Country(ies):** United Kingdom. Cloud Compute services will be run from a UK Data Centre (either Commercial or Government). Any other option is out of scope for this Framework (and would be governed by Oracle standard terms). Restricted Country : ✓☐ Location: United Kingdom **Data Centre Region Availability** Platform and data centre region availability information for Oracle Platform as a Service (PaaS) Cloud Services and for Oracle Infrastructure as a Service (IaaS) Cloud Services is provided on the Oracle Cloud Portal at REDACTED FOI 40
Standards:	In addition to complying with Clause 6.2 of the Call-Off Terms, including those Standards set out in Attachment 4 (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
Service Level Agreement or SLA:	The relevant service levels and availability criteria applicable to each of the Services provided under this Contract are as set out or referred to in Attachment 2 (Service Level Agreement(s)).
Services Suspension:	Notwithstanding any provisions of the AUP (set out in Attachment 7 (Supplier's Acceptable Use Policy) to this Order Form and/or any other Applicable Supplier Terms, the Supplier may only suspend the Buyer's and any Buyer User's access and use of all or the affected part of the Services where and to the extent it is entitled to do so and strictly in accordance with the provisions of Clause 14 (Suspension) of the Call-Off Terms.
On-boarding:	The on-boarding for the Contract is the responsibility of the Buyer except as stated here: Not Applicable
Off-boarding:	The off-boarding for the Contract is the responsibility of the Buyer except as stated here*:* Not applicable in accordance with Section 14 of the Product Terms. The retention period for Buyer Content set out in Clause 17.3.2(b) of the Call-Off Terms shall be amended from 60 (sixty) days: The retention period remains as sixty (60) days.

	Save where expressly agreed as a Special Term and set out in this Order Form and subject to reimbursement of reasonable charges in accordance with Clause 17.3.2(b) of the Call-Off Terms, where the Buyer terminates the contract for material Default, the Supplier may not charge the Buyer and/or any Buyer User any fees, costs or expenses relating to: (a) the Buyer's and/or any Buyer User's extraction, transfer and/or destruction of Buyer Content whenever and howsoever after such termination; or the Supplier complying with its exit related obligations under the Contract.
Licence Terms:	In accordance with and subject always to the minimum licence terms set out in Clause 9.4 of the Call-Off Terms, the Supplier's licence terms taken from the Applicable Supplier Terms are set out or referred to in Attachment 1 under the heading "Product Terms". Where relevant licence terms are not set out or referred to in Attachment 1 (Service Descriptions and Product Terms) to this Order Form under the heading "Product Terms", a licence meeting the minimum requirements set out in Clause 9.4 of the Call-Off Terms shall be deemed to be granted by the Supplier to the Buyer and any Buyer Users to enable it to receive and use the Services.
Force Majeure:	In respect of a Force Majeure event, the reference to 20 Working Days set out in Clause 21.4 of the Call-Off Terms shall be shortened to: Not applicable
Audit:	In addition to the audit rights set out in Clause 12 of the Call-Off Terms, the following additional audit rights shall apply to the Contract: As stated in Section 15 of the Product Terms The Supplier shall not require any Buyer to disapply its audit rights under Clause 12 of the 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 payment profile for this Contract is as set out in Attachment 3 (Charges and Payment Profile) to this Order Form. The charges will reflect the Buyer's actual consumption utilisation subject to the Funded Allocation Model Terms as set out in the Minimum Commitment section of the Order Form.
Charges breakdown:	The breakdown of the Charges is as set out in Attachment 3 (Charges and Payment Profile) to this Order Form
Currency:	All prices under this Contract shall be quoted exclusively in: **Pound Sterling** unless otherwise agreed in writing by the Buyer Authorised Representative. All Charges shall be paid and/or payable exclusively in Pounds Sterling.

Crown Commercial Service

Currency and currency conversion mechanism:	Not applicable
Payment method:	The payment method for this Contract is by electronic transfer to Suppliers nominated account by BACS. Any purchase order from the Buyer must include the following information: • Order Reference Number: REDACTED FOI 43 • Total Price In issuing a purchase order, You agree that no terms included in any such purchase order shall apply to the Services ordered under this Order Form.
Payment profile:	The payment profile for this Contract is as set out in Attachment 3 (Charges and Payment Profile) to this Order Form. Unless otherwise stated payment will be monthly in arrears. The charges will reflect the Buyer's actual consumption utilisation in accordance with the Funded Allocation Mode Terms as set out the Minimum Commitment Section to this Order Form...
Invoice details and frequency:	The Supplier will issue an invoice (including any Electronic Invoices) on a monthly basis in arrears. Pursuant to Clause 7.4 of the Call-Off Terms, the Buyer will pay the Charges to the Supplier within *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 43
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 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:	This is a consumption charge-based service, the total potential value of the Contract is £750,000.00 exclusive of VAT.
Applicable Discounts:	Pursuant to Clause 7.3 of the Call-Off Terms, the details of any applicable discounts and/or preferential pricing are as follows: Not Applicable
Minimum Commitments:	This is a consumption charge-based service. The Buyer will pay charges for the Services in accordance with the consumption as described below: REDACTED IN FULL

Additional Buyer terms:

Liability:	Not applicable
Buyer specific amendments to/ refinements of the Contract terms:	REDACTED IN FULL
Personal Data and Data Subjects:	See Attachment 5 (Schedule of Processing, Personal Data and Data Subjects) to this Order Form.

Alternative Clauses:

The following Alternative Clauses will apply:	Not Applicable

Crown Commercial Service

Section C - Commercially Sensitive information:

Commercially Sensitive information:

Any information that the Supplier considers sensitive for the duration of 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

For and on behalf of the Supplier:

Name:	REDACTED FOI 40
Job role/title:	REDACTED FOI 40
Signature:	REDACTED FOI 40
Date:	10-February-2023

For and on behalf of the Buyer:

Name:	REDACTED FOI 40
Job role/title:	REDACTED FOI 40
Signature:	REDACTED FOI 40
Date:	10th February 2023 .

Schedule A to the Order Form – Service Recipients

None

Crown Commercial Service

Attachment 1 – Service Descriptions and Product Terms

SERVICE DESCRIPTIONS:

See the relevant Service Description applicable to the Services purchased under this Order Form available at:

- **Oracle PaaS and IaaS Universal Credits Service Descriptions Effective Date: 08-December-2022** REDACTED FOI 40 -

- **Oracle Platform as a Service and Infrastructure as a Service – Public Cloud Service Descriptions Metered & Non-Metered Effective Date: 10-June-2022** ("**OCI Services Service Descriptions**"). REDACTED FOI 40

The OCI Services Service Descriptions are subject to change for 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:

As set in in the "Product Terms – Licence Terms" sub-section below, and in the Applicable Supplier Terms **Exhibit A (Oracle Product Terms)** to this Attachment 1 (Service Descriptions and Product Terms).

For the avoidance of doubt, of the order of precedence in respect of a conflict between the Call-Off Terms and the Applicable Supplier Terms, the Call-Off Terms takes precedence in accordance with section 2.2 and subsection 2.2.3 of the Call-Off Terms.

Product Terms – Licence Terms

Clause 9.4 of the Call Off Contract is applicable subject only to clause 6.1 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

Exhibit A – Oracle Product Terms

These Terms represent the Product Terms as envisaged by Framework Contract RM6111 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 RM6111, 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.

5.4. 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 6.1 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 8.4.2 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 8.1 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 9.6 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 9.8 of the Call Off Contract 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 9.6 – 9.10 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

If the Buyer exercises the right in clause 16.1 and clause 17.4.2, it has been agreed between the Parties that clause 17.4.2 (a) shall be applicable.

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 21 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 Cloud Hosting and Delivery Policy will apply (see **Appendix 1**) as will the Oracle Services Privacy Policy (see **Appendix 2**).

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 is available at https://www.oracle.com/a/ocom/docs/corporate/bcr- privacy-code-051719.pdf

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 3 (TUPE)** shall apply.

21. DEFINITIONS

21.1. 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: (a) the Oracle Cloud Hosting and Delivery Policies (see **Appendix 1**), the Program Documentation available on the Oracle website, the Service Descriptions incorporated into Your Call Off Contract, and the Data Processing Agreement incorporated into the Call Off Contract; and (b) Oracle's privacy policies. The following do not apply to any Oracle Software: the Oracle Cloud Hosting and Delivery Policies, the Service Descriptions, and the Data Processing Agreement.

"**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.

Crown Commercial Service

APPENDIX 1 TO EXHIBIT A (ORACLE PRODUCT TERMS)

ORACLE'S CLOUD HOSTING AND DELIVERY POLICY

OVERVIEW

These Oracle Cloud Hosting and Delivery Policies (these "**Delivery Policies**") describe the Oracle Cloud Services ordered by You. These Delivery Policies may reference other Oracle Cloud policy documents; any reference to "Customer" in these Delivery Policies or in such other policy documents shall be deemed to refer to "You" as defined in Your order. References in these Delivery Policies to a Cloud Services' "data center region" refers to the geographic region listed in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services. In addition, for purposes of the data center region listed in Your order, or selected when activating the production instance of Your Service, "Europe" refers to the member countries of the European Union, the United Kingdom, and Switzerland, collectively. Capitalized terms that are not otherwise defined in these Delivery Policies shall have the meaning ascribed to them in the Oracle agreement, Your order or the policy, as applicable. The Oracle Cloud Hosting and Delivery Policies are generally updated on a biannual basis.

Oracle Cloud Services are provided under the terms of the Oracle agreement, Your order, and Service Specifications applicable to such services. Oracle's delivery of the Oracle Cloud Services is conditioned on Your and Your users' compliance with Your obligations and responsibilities defined in such documents and incorporated policies. These Delivery Policies, and the documents referenced herein, are subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of performance, functionality, security, or availability of the Oracle Cloud Services provided during the Services Period of Your order.

Oracle Cloud Services are deployed at data centers or third-party infrastructure service providers retained by Oracle, with the exception of Oracle Cloud at Customer Services. Oracle Cloud at Customer Services are Public Cloud Services that are deployed at Your data center or at a third-party data center retained by You. You may purchase these services standalone or they may be deployed as the underlying platform for other Oracle Cloud Services. For Oracle Cloud at Customer Services, Oracle will deliver to Your data center certain hardware components, including gateway equipment, needed by Oracle to operate these services. You are responsible for providing adequate space, power, and cooling to deploy the Oracle hardware (including gateway equipment) and for ensuring adequate network connectivity for Oracle Cloud Operations to access the services. Oracle is solely responsible for maintenance of the Oracle hardware components (including gateway equipment).

These Delivery Policies do not apply to Oracle BigMachines Express, Oracle ETAWorkforce, or such other Oracle Cloud offerings as specified by Oracle in Your order or the applicable Service Specifications.

Crown Commercial Service

1. ORACLE CLOUD SECURITY POLICY

1.1 Oracle Information Security Practices – General

Oracle has adopted security controls and practices for Oracle Cloud Services that are designed to protect the confidentiality, integrity, and availability of Your Content that is hosted by Oracle in Your Oracle Cloud Services environment and to protect Your content from any unauthorized processing activities such as loss or unlawful destruction of data. Oracle continually works to strengthen and improve those security controls and practices.

Oracle Cloud Services operates under practices which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected. Oracle Cloud Services are aligned with National Institute of Standards and Technology ("NIST") 800-53 and 800-171.

Oracle Cloud information security practices establish and govern areas of security applicable to Oracle Cloud Services and to Your use of those Oracle Cloud Services. Oracle personnel (including employees, contractors, and temporary employees) are subject to the Oracle information security practices and any additional policies that govern their employment or the services they provide to Oracle.

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

For those Oracle Cloud Services which enable You to configure Your security posture, unless otherwise specified, You are responsible for configuring, operating, maintaining, and securing the operating systems and other associated software of these select Oracle Cloud Services (including Your Content) that is not provided by Oracle. You are responsible for maintaining appropriate security, protection, and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and the routine archiving of Your Content.

1.2 Physical Security Safeguards

Oracle employs measures designed to prevent unauthorized persons from gaining access to computing facilities in which Your Content is hosted such as the use of security personnel, secured buildings, and designated data center premises. Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Oracle controlled co-locations/data centers currently include, for example:

- Physical access requires authorization and is monitored
- All employees and visitors must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed while onsite
- Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards

Additional physical security safeguards are in place for Oracle-controlled Cloud data centers, which currently include safeguards such as:

- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles
- Entrances are manned twenty-four (24) hours a day, three-hundred-sixty-five (365) days a year by security guards who perform visual identity recognition and visitor escort management
- Safeguards related to environmental hazards
- Any physical movement of equipment is controlled by hand-delivered receipts and other authorized change control procedures

- Network cables are protected by conduits and, where possible, avoid routes through public areas.

This section does not apply to Oracle Cloud at Customer Services. You must provide Your own secure computing facilities for the hosting and operation of the Oracle Cloud at Customer Services-related hardware (including the gateway equipment) and network connections required for Oracle to provide the Oracle Cloud at Customer Services.

1.3 System Access Controls

Oracle may, depending upon the particular Cloud Services ordered, apply among others the following controls: authentication via passwords and/or multi-factor authentication, documented authorization and change management processes, and logging of access. All remote access to the Oracle Cloud Network by Oracle personnel that have access to Your Content must be through a Virtual Private Network, utilizing multi- factor authentication. Oracle prohibits (through both policy and technical controls) the use of personal devices to access the Oracle Cloud Network and the Services environment for the Cloud Services.

For Cloud Services hosted at Oracle: (i) log-ins to Cloud Services environments are logged and (ii) logical access to the data centers is restricted and protected.

1.4 Data Access Controls

For service components managed by Oracle, Oracle's access to Your Content is restricted to authorized staff.

With respect to Oracle personnel accessing the Services environment for the Cloud Services (including Your Content residing in the Cloud Services), Oracle enforces Role Based Access Controls (RBAC) and employs the access management principles of "need to know", "least privilege" and "segregation of duties." In addition, Oracle provides a mechanism by which You control Your access to Your Cloud Services environment and to Your Content by Your authorized staff.

1.5 User Encryption for External Connections

Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128 bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each version of Oracle Cloud Services will be made available via a portal accessible to You or in the corresponding Service Specifications for the Oracle Cloud Services. In some cases, a third party site that You wish to integrate with the Oracle Cloud Services, such as a social media service, may not accept an encrypted connection. For Oracle Cloud Services where HTTP connections with the third party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.6 Input Control

The source of Your Content is under Your control and Your responsibility, and integrating Your Content into the Cloud Services environment, is managed by You.

1.7 Data and Network Segregation

Your Content is logically or physically segregated from the content of other customers hosted in the Oracle Cloud Services environments. All Oracle Public Cloud networks are segregated from Oracle's Corporate networks.

1.8 Confidentiality and Training

Oracle personnel that may have access to Your Content are subject to confidentiality agreements. All Oracle personnel that have access to Your Content are required to complete information-protection awareness training upon hiring. Thereafter, all Oracle personnel that have access to Your Content must complete training in accordance with applicable Oracle security and privacy awareness training documentation.

1.9 Asset Management

Oracle is responsible for the protection and inventory of Oracle's Cloud Services assets. The responsibilities may include reviewing and authorizing access requests to those who have a business need and maintaining an inventory of assets.

You are responsible for the assets You control that utilize or integrate with the Oracle Cloud services, including: determining the appropriate information classification for Your Content, and whether the documented controls provided by Oracle Cloud Services are appropriate for Your Content. You must have or obtain any required consents or other legal basis related to the collection and use of information provided by data subjects, including any such consents or other legal basis necessary for Oracle to provide the Cloud Services.

1.10 Oracle Internal Information Security Policies

Oracle Cloud information security policies establish and govern areas of security applicable to Oracle Cloud Services and to Your use of Oracle Cloud Services. Oracle personnel are subject to the Oracle Corporate Information Security Policies and any additional policies that govern their employment or the services they provide to Oracle. Oracle's Information Security Program ("ISP") is comprised of documented policies that consider risk factors including cyber and security factors, with accompanying derivative procedures, standards and guidelines required for the effective operationalization of policy. Oracle's ISP is designed to ensure the confidentiality, integrity, privacy, continuity and availability of Your Content that is hosted by Oracle in Your Oracle Cloud Services through effective security management practices and controls. Oracle's ISP is reviewed annually by the Oracle Security Oversight Committee and updated as required.

1.11 Internal Security Reviews and Enforcement

Oracle employs internal processes for regularly testing, assessing, evaluating and maintaining the effectiveness of the technical and organizational security measures described in this section.

1.12 External Reviews

Oracle may conduct independent reviews of Cloud Services utilizing third parties in the following areas (the scope of any such reviews may vary by service and country):

- SOC 1 (based on Statement on Standards for Attestation Engagements (SSAE) No 18) and/or SOC 2 reports
- Other independent third-party security testing to review the effectiveness of administrative and technical controls.

Relevant information from these reviews may be made available to customers.

1.13 Oracle Software Security Assurance

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products and services, including the Oracle Cloud Services. The OSSA program is described at as follows

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience.

Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

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

1.14 Security Logs

Logs are generated for security-relevant activities on operating systems. Systems are configured to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors. Oracle reviews logs for forensic purposes and incidents; identified anomalous activities feed into the incident management process. Security logs are stored within the Security Information and Event Management system in a native, unaltered format and retained in accordance with Oracle's internal policies. Such logs are retained online for a minimum of ninety (90) days, or as otherwise required by an applicable regulatory framework.

1.15 Other Customer Security Related Obligations

You are responsible for:

- Implementing Your own comprehensive system of security and operational policies, standards and procedures, according to Your risk-based assessments and business requirements
- Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to the Oracle Cloud Services
- Managing client device security controls, so that antivirus and malware checks are performed on data or files before importing or uploading data into the Oracle Cloud Services
- Maintaining Customer-managed accounts according to Your policies and security best practices
- Additionally, for Oracle Cloud at Customer Services, You are responsible for the following:
- Adequate physical and network security

- Security monitoring to reduce the risk of real time threats and prevent unauthorized access to Your Oracle Cloud Services from Your networks; this includes intrusion detection systems, access controls, firewalls and any other network monitoring, and any management tools managed by You.

2. ORACLE CLOUD SERVICE CONTINUITY POLICY

2.1 Oracle Cloud Services High Availability Strategy

Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and/or storage.

2.2 Oracle Cloud Services Backup Strategy

Oracle periodically makes backups of Your production data in the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services, and may also be stored at an alternate location for retention purposes. A backup is typically retained online or offline for a period of at least sixty (60) days after the date that the backup is made. Oracle typically does not update, insert, delete or restore Your data on Your behalf. However, on an exception basis and subject to written approval, Oracle may assist You to restore data which You may have lost as a result of Your own actions.

For Oracle Cloud Services which enable You to configure backups in accordance with Your own policies, You are responsible for performing backups and restores of Your data, non-Oracle software, and any Oracle software that is not provided by Oracle as part of these services. Additionally, You are encouraged to develop a business continuity plan to ensure continuity of Your own operations in the event of a disaster.

3. PROVISIONS SPECIFIC TO PAAS AND IAAS

3.1 Oracle Information Security Practices – General

For the Oracle Video Plus (formerly Sauce mobile client) component of the Oracle Content and Experience Cloud Service – Advanced Video Management, the second paragraph of section 1.1 of the Oracle Cloud Hosting and Delivery Policies regarding alignment with ICO/IEC 27002 Code of Practice does not apply.

Physical Security Safeguards For the Oracle Apiary Cloud Service, Oracle Container Pipelines Cloud Service, Oracle Cloud Infrastructure - Ravello Service, Oracle CASB Cloud Services, and the Oracle Video Plus (formerly Sauce mobile client) component of the Oracle Content and Experience Cloud Service – Advanced Video Management, the following applies in lieu of the text in section 1.2 of the Oracle Cloud Hosting and Delivery Policies: In accordance with reasonable practices, Oracle provides secured computing facilities for both office locations and production Cloud infrastructure.

Crown Commercial Service

APPENDIX 2 TO EXHIBIT A (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 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. 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.

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 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. 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 Model Clauses or other adequate transfer mechanism as required under relevant data protection.

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**"), Switzerland, or the United Kingdom ("**UK**"), such transfers are subject to Oracle's Binding Corporate Rules for Processors (BCR-P) or the terms of the EU Model Clauses.

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 six (6) 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 (12) 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 (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. 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 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. You may consult with your Oracle services contact for additional information on data deletion prior to service completion.

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 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.

For personal information contained in Systems Operations Data collected in the EU, our legal basis for processing such information is our legitimate interest in performing, maintaining and securing our products and services and operating our business in an efficient and appropriate manner. Personal information may also be processed based on our legal obligations or legitimate interest to comply with such legal obligations.

2. Sharing Personal Information

Personal information contained in Systems Operations Data may be shared throughout Oracle's global organization. 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 organisational 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.

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 Model Clauses.

4. Security

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

5. User choices

To the extent provided under applicable laws, Users may request to access, correct, update or delete personal information contained in Systems Operations Data in certain cases, or otherwise exercise their choices with regard to their personal information by filling out an inquiry form.

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 Data Protection 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 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, written inquiries to the EU Data Protection Officer may be addressed to:

REDACTED FOI 40
Hauptstraße 4
D-85579 Neubiberg / München
Germany
Email: REDACTED FOI 40

3. Dispute resolution or filing a complaint

If You or a User have any complaints regarding our compliance with our privacy and security practices, please contact us first. We will investigate and attempt to resolve any complaints and disputes regarding our privacy practices.

Under certain conditions, Users may invoke binding arbitration when other dispute resolution procedures have been exhausted. 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 October 20, 2020. However, the Services Privacy Policy can change over time, for example to comply with legal requirements or to meet changing business needs.

Crown Commercial Service

APPENDIX 3 TO EXHIBIT A (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.

Crown Commercial Service

Attachment 2 – Service Level Agreement(s)

These are contained in:

(a) section 3 to the document entitled "*Oracle Cloud Hosting and Delivery Policies*" (available at REDACTED FOI 40 **("Oracle Cloud Hosting and Delivery Policies")** ; and

(b) sections 1 and 2 inclusive in the document entitled "*Oracle PaaS and IaaS Public Cloud Services – Pillar document*" (available at REDACTED FOI 40 **Oracle PaaS and IaaS Public Cloud Services Pillar Document")**. These sections also describe the applicable service credit regime and the process for claiming service credits.

Oracle's Cloud Hosting and Delivery Policies and Oracle PaaS and IaaS Public Cloud Services Pillar Document are subject to change for 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.

Crown Commercial Service

Attachment 3 – Charges and Payment Profile

Offer Validity: This order is valid through 28-Feb-2023 and shall become binding upon execution by the Buyer and acceptance by the Supplier.

New Subscription

Service Period: 12 months					
Cloud Services	**Data Center Region**	**Period**	**Quantity**	**Term**	**Funded Allocation Value**
B88206 - Oracle PaaS and IaaS Universal Credits	Customer Selected	Annual	£750000	12 months	£750,000.00
				Subtotal	£750,000.00

Fee Description	Net Fee
Cloud Services Fees	0.00
Net Fees	0.00
Funded Allocation Value	£750,000.00
Total Fees	0.00

Rate Card Pricing for IaaS/PaaS Public Cloud Services

B88206 - Oracle PaaS and IaaS Universal Credits

Cloud Service Category Discounts

REDACTED IN FULL

Crown Commercial Service

Attachment 4 – Schedule of Standards

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 data centres used 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 5 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 5 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 5 shall be with the Buyer at its absolute discretion.

1. The contact details of the Buyer's Data Protection Officer are: REDACTED FOI 40 **DWP Data Protection Team, Benton Park View 6, Room BP6001, Mail Handling Site A, Wolverhampton, WV98 1ZX,** REDACTED FOI 40
2. The contact details of the Supplier's Data Protection Officer are: REDACTED FOI 40 **Hauptstraße 4 D-85579 Neubiberg / München Germany Email:** REDACTED FOI 40
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 5.

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 Call-Off Terms.
Subject matter of the processing:	See below under Type of Personal Data and Categories of Data Subject.
Duration of the processing:	For the duration of the Contract Period.
Nature and purposes of the processing:	Nature: organisation, structuring and storage of data Purposes: • providing the Cloud Services in accordance with the applicable Agreement, Oracle Cloud DPA, Service Specifications, and order for Services, • complying with Buyer documented written instructions, and/or • complying with Supplier's regulatory obligations.
Type of Personal Data being Processed:	• personal contact information such as name, address, telephone or mobile numbers, email address and passwords; • information concerning individual data subjects and their family including age, date of birth, marital status, number of children and name(s) of spouse and/or children; • employment details including employer name, job title

	and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; • financial details; • goods and services provided;
Categories of Data Subject:	Buyer representatives and end users, job applicants, contractors, collaborators, partners, suppliers, customers and clients.
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)**	Following termination the Supplier will return or otherwise make available for retrieval Buyer Personal Data then available in Buyer Cloud Services environment, unless otherwise expressly stated in the Service Specifications. For Cloud Services for which no data retrieval functionality is provided by Supplier as part of the Cloud Services, the Buyer is advised to take appropriate action to back up or otherwise store separately any Personal Data while the production Cloud Services environment is still active prior to termination.

Crown Commercial Service

Attachment 6 – Alternative Clauses

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 31.1 and 31.5 of the Call-Off Terms):

(a) References to "*England and Wales*" in the original Clauses 31.1 and 31.5 of the 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 31.1 and 31.5 of the Call-Off Terms):

(a) References to "England and Wales" in the original Clauses 31.1 and 31.5 of the 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 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 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 6 (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 6, 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 6 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 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 6 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 6 shall not be subject to Clause 8.1 of the Call-Off Terms and the Supplier's liability under paragraph 4.4 of this Attachment 6 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 6 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 6 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 6 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 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 Call-Off Terms.

4.8. In addition to those circumstances listed in Clause 19.7 of the 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 6 and 4.6 of this Attachment 6.

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 6, 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 31 (Governing Law, Jurisdiction and Dispute Resolution) of the 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 6 shall be deemed to be an event to which Clause 16.2.1 of the 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 Call-Off Terms.

6. Data Protection and off-shoring

6.1. For the purposes of Clause 15.4.4 of the 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.

Crown Commercial Service

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 6. 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 Call-Off Terms applies.

Crown Commercial Service

Exhibit 1 to Attachment 6

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;

---

[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.

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.

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.

[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

[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 6

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: *CPQ-2658402-1* (('**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:	REDACTED FOI 40
FULL NAME:	REDACTED FOI 40
POSITION:	REDACTED FOI 40
COMPANY:	REDACTED FOI 40
DATE OF SIGNATURE:	10th February 2023

Crown Commercial Service

Attachment 7 – Acceptable Use Policy

1. The Buyer may not, and may not cause or permit others to: (a) use the Services to harass any person; cause damage or injury to any person or property; publish any material that is false, defamatory, harassing or obscene; violate privacy rights; promote bigotry, racism, hatred or harm; send unsolicited bulk e-mail, junk mail, spam or chain letters; infringe property rights; or otherwise violate applicable laws, ordinances or regulations; (b) perform or disclose any benchmarking or availability testing of the Services; (c) perform or disclose any performance or vulnerability testing of the Services without the Supplier's prior written approval, or perform or disclose network discovery, port and service identification, vulnerability scanning, password cracking or remote access testing of the Services; or (d) use the Services to perform cyber currency or crypto currency mining ((a) through (d) collectively, the "**Acceptable Use Policy**"). In addition to other rights that the Supplier has in the Supplier Product Terms, this Call-Off Contract and the Order Form, the Supplier has the right to take remedial action if the Acceptable Use Policy is violated, and such remedial action may include, without limitation, removing or disabling access to material that violates the Acceptable Use Policy.

Crown Commercial Service

Attachment 8 – Data Processing Agreement

1. 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/a/ocom/docs/corporate/data-processing-agreement-062619.pdf and is set out in Appendix A to this Attachment 8. 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

APPENDIX A to Attachment 8

Data Processing Agreement for Oracle Services
("Data Processing Agreement")

Version January 1, 2023

1. Scope and Applicability

This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

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

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

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

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

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

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

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

obligations which may apply to such data.

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

2.8 Oracle is a Service Provider in respect to Personal Information processed in performance of the Services. Oracle will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Services Agreement, including for any Commercial Purpose, or (ii) outside of the direct business relationship between Oracle and You; or (c) combine Personal Information received from or on behalf of You with Personal Information received from or on behalf of any third party, or collected from Oracle's own interaction with Individuals, except to perform a Business Purpose that is permitted by the CCPA and the Services Agreement. Oracle will notify You of its use of Subprocessors in accordance with Section 5 of this Data Protection Agreement; and ensure Subprocessors are subject to applicable written agreements per Section 5 of this Data Protection Agreement. The parties acknowledge that the Personal Information You disclose to Oracle is provided only for the limited and specified Business Purposes set forth in the Services Agreement. Oracle shall provide the same level of protection to Personal Information as required by the CCPA and as more fully set out in the Agreement. You may take such reasonable steps as may be necessary (a) to remediate Oracle's unauthorized use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this Data Processing Agreement by exercising Your rights under Section 8 of this Data Processing Agreement. Oracle shall notify You if it makes a determination that it is not able to meet its obligations under the CCPA in connection with its provision of the Services.

3. Your Instructions

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

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

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

4. Privacy Inquiries and Requests from Individuals

4.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by Oracle under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address

the request. Additional information on how to access the Services to address privacy requests or inquiries from Individuals is available in the applicable Oracle Product or Service Feature Guidance documentation available on My Oracle Support (or other applicable primary support tool or support contact provided for the Services).

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

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

5. Oracle Affiliates and Third Party Subprocessors

5.1 You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

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

5.3 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the NetSuite Support Portal or Your Oracle project manager). To receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, You can (i) sign up per the instructions on My Oracle Support, Document ID 2288528.1; or (ii) Oracle will provide you notice of intended changes where a sign up mechanism is not available. For ACS and Consulting Services, any additional Third Party Subprocessors that Oracle intends to use will be listed in Your order for ACS or Consulting Services, or in a subsequent "Oracle Subprocessor Notice", which Oracle will send to you by e-mail as necessary.

5.4 Within thirty (30) calendar days of Oracle providing such notice to You under Section 5.3 above, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services by submitting a "service request" via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. You and Oracle will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 5.4 only pertains to a portion of

Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

6. Cross-Border Data Transfers

6.1 For Cloud Services, Personal Information will be stored in the data center region specified in Your order for such Services or, if applicable, the geographic region that You have selected when activating the production instance of such Services.

6.2 Without prejudice to Section 6.1 above, Oracle may Process Personal Information globally as necessary to perform the Services, such as for support, incident management or data recovery purposes.

6.3 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable European Data Protection Law to countries outside Europe not covered by an adequacy decision, such transfers are subject to (i) Oracle's Binding Corporate Rules for Processors or BCR-p (also referred to as the Oracle Processor Code) and (ii) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021.

The most current version of Oracle's Binding Corporate Rules for Processors (Oracle Processor Code) is available on https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing, and is incorporated by reference into the Services Agreement and this Data Processing Agreement. Oracle has obtained EEA authorization for its Binding Corporate Rules for Processors (Processor Code) and will maintain such authorization for the duration of the Services Agreement. Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with Oracle's Binding Corporate Rules for Processors (Oracle Processor Code), the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021, this Data Processing Agreement and the Services Agreement.
6.4 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable UK Data Protection Law, to countries outside the United Kingdom not covered by an Adequacy Decision by the UK ICO, such transfers are subject to (i) the terms of Module 2 (Controller to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2021 as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (the "**IDTA**"), which are incorporated herein by reference; and (ii) when approved by the UK ICO, the approved UK Binding Corporate Rules for Processors, in the form that will be approved by the UK ICO for use in the UK and will be published on Oracle's public websites. The IDTA will be read in conjunction with the Agreement and the Data Processing Agreement.

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

6.6 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under other Applicable Data Protection Laws globally, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

7. Security and Confidentiality

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

- For **all Services:** Oracle's Corporate Security Practices, available at https://www.oracle.com/corporate/security-practices/;
- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: http://www.netsuite.com/portal/resource/terms-of-service.shtml;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: https://www.oracle.com/support/policies.html;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: http://www.oracle.com/us/corporate/contracts/consulting-services/index.html.

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

8. Audit Rights and Assistance with Data Protection Impact Assessments

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

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

8.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration,

and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

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

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

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

8.7 Without prejudice to the rights granted in Section 7.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

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

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

9. Incident Management and Breach Notification

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

9.2 Oracle will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible

adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

10. Return and Deletion of Personal Information

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

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

11. Legal Requirements

11.1 Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

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

11.3 To the extent Oracle is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on Oracle, including whether the request is consistent with Applicable Data Protection Law. Any request that is not legally valid and binding on Oracle will be resisted in accordance with applicable law.

12. Data Protection Officer

12.1 Oracle has appointed a Chief Privacy Officer and a local Data Protection Officer in certain countries. Further details on how to contact Oracle's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available here.

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

13. Definitions

"**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, including Applicable European Data Protection Law, Applicable UK Data Protection Law, the California Consumer Privacy Act as amended ("CCPA") and other US State laws.

"**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; and (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended.

"Applicable UK Data Protection Law" means (i) the UK GDPR, meaning the EU General Data Protection

Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 and the Data; and (ii) the UK Data Protection Act 2018, as amended.

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

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

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

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

"Service Provider", "Sell", "Share", "Business Purpose", and **"Commercial Purpose"** have the meaning set forth under the CCPA.

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

"**Oracle Intra-Company Data Transfer and Mandate Agreement"** means the Oracle Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

"**Oracle Binding Corporate Rules for Processors**" or "**Oracle Processor Code**" means the EU or UK Oracle's Privacy Code for Processing Personal Information of Customer Individuals, as the case may be.

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

"**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.

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

"**Services**" or the equivalent terms "Service Offerings" or "services" means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

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

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

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

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

Crown Commercial Service

Annex 1

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/RM6111 titled "*RM6111 Cloud Compute Template Call-Off Terms Final 1.1*" ("**Agreed Call-Off Terms**") and the Agreed Call-Off Terms v1.1 are incorporated in this Order Form by reference accordingly.

Crown Commercial Service

Annex 2
Applicability Matrix

	CCS – Framework Terms			Supplier - General Terms		Supplier - Service Specific	
	Call Off Contract	Order Form	Framework	Acceptable Use Policy	Data Protection Addendum	Service Level Agreement + Credits	Other Product Terms
Service Description	Cl.5	Front End + Attachment 1	Sch 2 + 'Catalogue'				Front End + Attachment 1
Service Levels	Cl.5	Front End + Attachment 2				Attachment 2	
Standards and data security	Cl.6 & 11	Attachment 4 + Attachment 1	Sch. 2				
Warranties	Cl.6	Attachment 1					
Data Protection	Cl.15	Attachments 5 and 8			Attachments 1 and 8		
Charges & invoicing	Cl.7	Front End + Attachment 3					
Liability	Cl.8	Front End + Attachment 1					
Confidentiality	Cl.19	Attachment 1					
IPR/licence	Cl.9	Front End					Licence terms (Attachment 1)
Suspension	Cl.14	Attachment 7		Attachment 7			
Term and termination	Cl.4, 16 & 17	Front End + Attachment 1					
Audit	Cl.12	Front End + Attachment 1					
Force Majeure	Cl.21	Attachment 1					
Subcontracting	Cl.18	Front End + Attachment 1			Attachments 1 and 8		
Transparency	Cl.20	Section C					

Boxes shaded: Teal = main source & Pale Green = secondary source