

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE: [Insert Buyer's contract reference number]

THE BUYER: [Insert Buyer's name]

BUYER ADDRESS [Insert business address]

THE SUPPLIER: Oracle Corporation UK Limited

SUPPLIER ADDRESS: Oracle Parkway, Thames Valley Park, Reading, Berkshire
RG6 1RA

REGISTRY: Companies House

REGISTRATION NUMBER: 01782505

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated as described in this Order Form.

The unique identifier (OCID) for this Framework is RM1557.15.

It's issued under the Framework with the reference number RM1557.15 for the provision of Software as a Service (SaaS) services and associated Professional Services.

CALL-OFF LOT(S):

Lot 2b: RM1557.15.2b

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms.
2. Joint Schedule 1 (*Definitions*) RM1557.15
3. Framework Special Terms
4. The Supplier Terms, subject to the provisions set out under the heading of "Applicability of Supplier Terms" in this Order Form.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

5. The following Schedules in equal order of precedence:
 - Joint Schedules for RM1557.15
 - Joint Schedule 2 (*Variation Form*)
 - Joint Schedule 3 (*Insurance Requirements*)
 - Joint Schedule 4 (*Commercially Sensitive Information*)
 - Joint Schedule 5 (*Sustainability*)
 - Joint Schedule 6 (*Key Subcontractors*)
 - Joint Schedule 7 (*Financial Difficulties*)
 - Joint Schedule 8 (*Guarantee*)
 - Joint Schedule 9 (*Rectification Plan*)
 - Joint Schedule 10 (*Processing Data*)
 - Call-Off Schedules for RM1557.15
 - Call-Off Schedule 1 (*Intellectual Property Rights*)
 - Call-Off Schedule 2 (*Staff Transfer*)
 - Call-Off Schedule 20 (*Call-Off Specification*)
 - Call-Off Schedule 27 (*Cyber Essentials Scheme*)
6. CCS General Terms for RM1557.15
7. Supplier Service Descriptions (if any), as long as any parts of the Supplier Service Descriptions that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above

APPLICABILITY OF SUPPLIER TERMS

Other than any Supplier Terms expressly set out under the heading of "Supplier Terms" in this Order Form, no Supplier or third party terms that may be provided or proposed by the Supplier will form part of the Call-Off Contract. That includes any such other terms that may be written on the back of, added to this Order Form, or presented at the time of delivery.

The Supplier Terms (if any) set out under the heading of "Supplier Terms" in this Order Form shall:

1. only be applicable to the Call-Off Contract to the extent that they directly relate to the permitted subject matter of the relevant Supplier Terms, as set out in the definitions of Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLA or Supplier Licence Terms (as applicable) in Joint Schedule 1 (*Definitions*); and
2. not be applicable to the Call-Off Contract (and shall be deemed to be ineffective) to the extent that they include:
 - a. any Additional Third Party Terms and/or Inapplicable Additional Terms;
 - b. any indemnities (or clauses of a similar nature to indemnities); and/or
 - c. any provisions which would have any material impact on:
 - i. the potential liability of either Party under the Call-Off Contract; and/or
 - ii. the balance of risks under the Call-Off Contract from the Buyer's perspective (including the creation of new or increased potential liabilities, new or materially different operational responsibilities for the Buyer and/or any Buyer Users and/or new or increased constraints on the Buyer's rights of termination),

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

in each case when compared to the other terms of the Call-Off Contract (i.e. other than the Supplier Terms) as listed under the heading of "Call-Off Incorporated Terms" in this Order Form.

SUPPLIER TERMS

The Supplier Terms (if any) applicable to this Call-Off Contract are as listed below.

Supplier Standard Terms

1. The Supplier Acceptable Use Policy listed below:

The Buyer may not, and may not cause or permit others to: (i) 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 intellectual or other property rights; sell, manufacture, market and/or distribute any product or service in violation of applicable laws; or otherwise violate applicable laws, ordinances or regulations; (ii) perform or disclose any benchmarking or availability testing of the Services; except as permitted in the Solution Descriptions; (iii) perform or disclose any performance or vulnerability testing of the Services without the Supplier's prior written approval, except as permitted in the Solution Descriptions, or perform or disclose network discovery, port and service identification, vulnerability scanning, password cracking or remote access testing of the Services; or (iv) use the Services to perform cyber currency or crypto currency mining; or (v) use the Services for any purpose other than their applicable Intended Purpose, ((i) through (v) collectively, the "Acceptable Use Policy"). In addition to other rights that we have in this Call-Off Contract, the Supplier has the right to take remedial action if the Acceptable Use Policy is violated, and such remedial action may, to the extent permitted by law, include removing or disabling access to material that violates the policy.

"Intended Purpose" has the meaning set out in the Supplier Licence Terms.

"Solution Descriptions" means the Solution Descriptions applicable to the Services ordered under Call-Off Schedule 20 (Call-Off Specification) of this Call-Off Contract and may be accessed at <http://www.oracle.com/contracts> on the Oracle Health tab.

2. The Supplier Data Processing Agreement listed below:

The version of the Data Processing Agreement applicable to this Call-Off Contract: (i) as attached to this Order Form which may be updated from time to time; (ii) as available at <https://www.oracle.com/contracts/#data-processing> or as otherwise notified by the Supplier to the Buyer; and (iii) will remain in force during the Call-Off Contract Period.

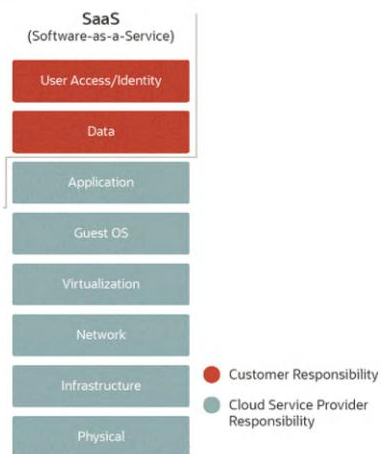
3. The Supplier Specific Shared Responsibility Model listed below:

The Supplier Specific Shared Responsibility Model applicable to this Call-Off Contract: (i) is illustrated below; and (ii) as further set out at [full details of Supplier Specific Shared Responsibility Model to be provided by the Supplier to the Buyer prior to entering a Call-Off Contract].

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

Shared Responsibility Security Model



Supplier Service Specific Terms

1. The Supplier SLA listed below:

The Supplier's service level terms shall be those applicable to the relevant Services as set out in the applicable Solution Descriptions available at <http://www.oracle.com/contracts> on the Oracle Health tab.

“**Solution Descriptions**” means the Solution Descriptions applicable to the Services ordered under Call-Off Schedule 20 (Call-Off Specification) of this Call-Off Contract and may be accessed at <http://www.oracle.com/contracts> on the Oracle Health tab.

2. The Supplier Licence Terms listed below:

The Supplier Licence Terms shall be comprised of: (i) the Supplier Licence Terms attached to this Order Form; and (ii) the terms set out in Call-Off Schedule 20 (Call-Off Deliverables).

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1

Notwithstanding any other provision of this Call-Off Contract, if there is a conflict between the Supplier Terms and any other term of this Call-Off Contract (including without limitation the Framework Special Terms), the Supplier Terms shall take precedence and the section titled 'Applicability of Supplier Terms' in this Order Form shall not apply.

CALL-OFF START DATE: **[Insert Day Month Year]**

CALL-OFF EXPIRY DATE: **[Insert Day Month Year]**

CALL-OFF INITIAL PERIOD: **[Insert Years, Months]**

**CALL-OFF OPTIONAL
EXTENSION PERIOD:** **[Insert Years, Months]**

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

CALL-OFF DELIVERABLES

Subject to Part A of Call-Off Schedule 20 (Call-Off Specification), Call-Off Deliverables are as detailed in Part B of Call-Off Schedule 20 (Call-Off Specification) in accordance with the Supplier Licence Terms.

The Services Period for the Services commences on the Call-Off Start Date. If no specific date is specified above, then the "Call-Off Start Date" for each Service will be the date that the Buyer is issued access that enables the Buyer to activate the Services.

All Services listed on this Order Form are provided by the Supplier under, and subject to, the Supplier Licence Terms and all Oracle documents referenced in those Supplier Licence Terms.

For Call-Off Contracts under Lot 2b, any proposed Service Modifications or proposed modifications to Supplier Service Specific Terms pursuant to Clauses 2.16 and/or 2.17 of the General Terms (those Clauses 2.16 and 2.17 having been inserted in the General Terms pursuant to Framework Special Term 15 as set out in the Framework Award Form) can be notified by the Supplier and dealt with solely in accordance with section [●] of the Supplier Licence Terms in this Call-Off Contract.

The Supplier shall provide notice of any proposed Service Modifications or proposed modifications to Supplier Service Specific Terms solely in accordance with section [●] of the Supplier Licence Terms in this Call-Off Contract.

SERVICE REQUEST PROCESS

The Buyer can provision and manage its Services in conjunction with the Client Account Executive ("CAE") allocated to this Call-Off Contract by the Supplier.

ANTICIPATED CONTRACT VALUE

[Insert anticipated total value of the Contract]

CALL-OFF CHARGES

Fee Description	Net Fee (£)
Services Fees	£[Insert]
Net Fees	£[Insert]
Total Fees	£[Insert]

The Buyer agrees to pay any sales, value-added or other similar taxes imposed by applicable law, except for taxes based on the Supplier's income.

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4 and 5 in Framework Schedule 3 (Framework Prices).

MINIMUM COMMITMENT(S)

The Buyer may not reduce the quantity of Services purchased hereunder (e.g., user or record counts, storage, etc.), in whole or in part, during the Services Period set forth below in Part B (Deliverables) to Call-Off Schedule 20 (Call-Off Specification). Section [●] of the Supplier Licence Terms sets out the Buyer's liability in the event of termination of this Call-Off Contract by the Buyer pursuant to Clause 13.2.2 of the General Terms.

CURRENCY CONVERSION MECHANISM (IF APPLICABLE)

N/A

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

INDEXATION

N/A

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

1. Payment Terms

- a. Net thirty (30) days from invoice date.
- b. The Buyer may only retain or set off any amount owed to it by the Supplier against any amount due to the Supplier under this Call-Off Contract. The Buyer's right to retain or set-off amounts owed to it shall only apply where the Supplier has agreed that the amount is owed or the Buyer have 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.
- c. The Supplier processes a Buyer's order after receipt of a purchase order. Any terms and conditions on the Buyer's purchase order are void and have no legal effect. Once placed, this Order Form is non-cancellable and the sums paid non-refundable, except as otherwise provided under in this section.

BUYER'S INVOICE ADDRESS:

[Insert name]

[Insert role]

[Insert email address]

[Insert address]

BUYER'S AUTHORISED REPRESENTATIVE

[Insert name]

[Insert role]

[Insert email address]

[Insert address]

PROGRESS REPORT FREQUENCY

N/A

PROGRESS MEETING FREQUENCY

N/A

INTELLECTUAL PROPERTY RIGHTS

In accordance with Clause 10.4 of the General Terms, the IPR Option that is applicable to this Call-Off Contract is set out in the Framework Award Form.

Notwithstanding any other provision of this Call-Off Contract, the intellectual property rights applicable to this Call-Off Contract are set out in section [●] of the Supplier Licence Terms attached to this Order Form.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

MAXIMUM LIABILITY

Subject to sections [●] of the Supplier Licence Terms, the limitation of liability for this Call-Off Contract is stated in Clause 14.2 of the General Terms (as that Clause 14.2 has been amended pursuant to Framework Special Term 12 as set out in the Framework Award Form), except that under Clause 14.2(a) of the General Terms, the £500,000 alternative cap on liability under Lot 2b shall not apply as set out at section [●] of the Supplier Licence Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **[Insert Estimated Charges in the first 12 months of the Contract. The Buyer must always provide a figure here]**

BUYER'S ENVIRONMENTAL POLICY

See Clause 33 of the General Terms

ADDITIONAL INSURANCES

N/A

COMMERCIALLY SENSITIVE INFORMATION

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
5	Any	Information not in the public domain relating to any litigation or disputes that the Supplier group is a party to.	Indefinitely

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

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

ADDITIONAL KEY SUBCONTRACTOR(S)

N/A

ADDITIONAL AUTHORISED SUBPROCESSORS (Lot 1a/Lot 1b only)

N/A

GUARANTEE

N/A

ICT POLICY (IF APPLICABLE)

N/A

PRODUCT ROADMAP (IF APPLICABLE)

N/A

QUALITY PLANS

N/A

MAINTENANCE OF THE ICT ENVIRONMENT

N/A

KEY STAFF AND KEY ROLES

N/A

BUYER'S SECURITY REQUIREMENTS AND ICT POLICY SECURITY REQUIREMENTS (IF APPLICABLE)

N/A

STAFF VETTING REQUIREMENTS (ALL LOTS OTHER THAN LOT 1B)

Details of staff vetting undertaken by the Supplier are set out in [●] of the Supplier Licence Terms attached to this Order Form.

SECURITY ASPECTS LETTER (LOT 1A AND LOT 1B ONLY)

N/A

Framework Ref: RM1557.15

Project Version: v1.1

Model Version: v1.0 PA

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2025

CYBER ESSENTIALS CERTIFICATION

Cyber Essentials Scheme Certificate

SPECIFIC EXIT MANAGEMENT ASSISTANCE (LOT 1A AND LOT 1B ONLY)

N/A

VIRTUAL LIBRARY

N/A

SERVICE CREDITS

- **Service Credits:** will accrue in accordance with the Supplier's published service credit regime for the Service in question.
- **The Service Credit Cap is:** the maximum monthly service credits that can accrue under the Supplier's published service credit regime for the Service in question.
- **The Service Period is:** One Month
- **A Critical KPI Failure is:** Not applicable

SUPPLIER'S AUTHORISED REPRESENTATIVE

[Insert name]

[Insert role]

[Insert email address]

[Insert address]

SUPPLIER'S CONTRACT MANAGER

[Insert name]

[Insert role]

[Insert email address]

[Insert address]

SOCIAL VALUE COMMITMENT

N/A

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2025

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

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

These terms form part of a Call-Off Contract entered into between Oracle and the Buyer identified in a relevant Order Form pursuant to the Framework Contract. Words or phrases used in this document which are defined in the Call-Off Contract have the same meaning when used in this Data Processing Agreement.

References to the Services Agreement are to the Call-Off Contract. References in this Data Processing Agreement to "Oracle Health", "we", "us" or "our" are references to Oracle Corporation UK Limited and references to "You" or "Your" are to the Buyer identified in the Order Form.

1. Scope, Order of Precedence and Applicability

1.1 This Data Processing Agreement applies to Oracle Health'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. This Data Processing Agreement also applies to any future contracted Services, which Oracle Health provides to You and to all other activities in which employees of Oracle Health come into contact with, or may come into contact with Your Personal Information as part of the provision of Services, or when the possibility of this cannot be ruled out.

1.2 Except as expressly stated otherwise in this Data Processing Agreement or Your Services Agreement, in the event of any conflict between the terms of the Services Agreement, including any policies or schedules referenced therein, and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall take precedence.

2. Controller and Processor of Personal Information and Purpose of Processing

2.1 You are the Controller and Oracle Health 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 Health and any persons acting under the authority of Oracle Health, including any Oracle Health Affiliates and Third Party Subprocessors as set forth in Section 7, will Process Personal Information solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

3. Categories of Personal Information and Data Subjects

3.1 In order to perform the Services and depending on the Services You have ordered, Oracle Health may Process some or all of the following categories of Personal Information: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle, medical social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; medical treatment details including diagnosis, medication, condition; 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.

3.2 Categories of Data Subjects whose Personal Information may be Processed in order to perform the Services may include, among others, in-patients and out-patients, medical staff (referring, treating and post-treatment physicians), relatives and contact persons of patients, accompanying persons, staff of rescue and transport services, other employees of the hospital, suppliers / sales representatives, Your representatives and end users, such as Your employees, contractors, collaborators, partners,

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

suppliers, customers and clients.

3.3 Additional or more specific categories of Personal Information and/or Data Subjects may be described in the Services Agreement. Unless necessary for the Services specified in the Services Agreement, You may not disclose to or otherwise provide Oracle Health with any sensitive or special category Personal Information that imposes specific data security or data protection obligations on Oracle Health in addition to or different from those specified in the Data Processing Agreement or Services Agreement.

4. Your Instructions

4.1 Oracle Health will Process Personal Information on Your written instructions as specified in the Services Agreement and this Data Processing Agreement.

4.2 To the extent required by Applicable Data Protection Law, Oracle Health will inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. After giving such notice, Oracle Health is entitled to suspend the implementation of the relevant instruction, until You have either confirmed or modified the instruction. You acknowledge and agree that Oracle Health is not responsible for performing legal research and/or for providing legal advice to You.

4.3 You shall bear all additional expenses incurred as a result of any additional instruction not agreed under the Service Agreement in accordance with the terms of the Service Agreement, unless the instruction was directed at complying with a legal obligation to which only Oracle Health is subject. To the extent Oracle expects to incur significant 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.

5. Rights of Data Subjects

5.1 You control access to Your Services environment that holds Personal Information about Your end users, patients and other data subjects' Personal Information processed in Your systems. All Data Subjects should direct any requests related to their rights under Applicable Data Protection Law to You.

5.2 To the extent such access is not available to You, Oracle will provide assistance with requests from Data Subjects to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to processing related to Personal Information held in Your Services environment on Oracle Health systems, insofar as reasonably and technically possible.

5.3 If Oracle Health directly receives any requests or inquiries from Data Subjects that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Data Subject.

6. Transfers

6.1 Oracle Health will not disclose any Personal Information You have disclosed or accessed in the course of Oracle Health rendering Services to a third-party without Your prior written approval, unless such disclosure is mandated by laws applicable to Oracle Health. Oracle Affiliates acting as subprocessors and Third-Party Subprocessors as specified in Section 7 are not regarded as third parties under this Data Processing Agreement.

6.2 Oracle Health may access and Process Personal Information on a global basis as necessary to perform the Services, including for IT security purposes, maintenance and performance of the Services and related infrastructure, Services technical support and Service change management.

6.3 To the extent such global access under Section 6.2 involves a transfer of Personal Information subject to cross-border data transfer restrictions under Applicable European Data Protection Law to

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

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 3 (Processor to Processor) of the EU Standard Contractual Clauses 2021/914 of 4 June 2022, unless You instruct Oracle Health otherwise.

The most current version of the Oracle Processor Code is available on <https://www.oracle.com/contracts/cloud-services/>, and is incorporated by reference into the Services Agreement and this Data Processing Agreement. Oracle has obtained EEA authorization for its Processor Code and will maintain such authorization for the duration of the Services Agreement.

6.4 To the extent such global access under Section 6.2 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 applicable terms 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, Oracle's 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 Services Agreement and the Data Processing Agreement.

6.5 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. Oracle Affiliates and Third Party Subprocessors

7.1 Subject to the terms and restrictions specified in Sections 2.2, 6 and 7, You provide Oracle Health general written authorization to engage Oracle Affiliates and Third Party Subprocessors to assist in the performance of the Services.

7.2 To the extent Oracle Health 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 Health under the terms of this Data Processing Agreement and Applicable Data Protection Law. Oracle Health maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists may be made available to You via (i) the applicable primary support tool provided for the Services, such as the Oracle Health Cerner Data Protection Portal; (ii) upon request via Your support contact or (iii) on a publicly available website. If You would like to receive notice of any intended changes to these lists, You can sign up to receive notifications or Oracle will provide you notice of intended changes where a sign-up mechanism is not available.

7.3 Within thirty (30) calendar days of Oracle Health providing such notice, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Information in accordance with this Data Processing Agreement or Applicable Data Protection Law in writing by submitting a "service request" via the applicable primary support tool or process provided for the Services. In the event Your objection is justified, You and Oracle Health 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 Subprocessors' or Oracle Affiliate's compliance with this 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 Health 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 and Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

termination in accordance with this Section 7.3 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

7.4 Oracle remains responsible at all times for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

7.5 Any services provided by Third Parties which, by design, do not access or otherwise Process Personal Information, are excluded from the scope of this Data Processing Agreement. These Third Parties are not subprocessors nor subcontractors as they do not Process Personal Information on behalf of Oracle Health as part of the Services.

8. Technical and Organizational Measures, and Confidentiality of Processing

8.1 Oracle Health has implemented and will maintain appropriate Technical and Organizational security Measures ("TOMs") for the Processing of Personal Information. These measures take into account the nature, scope and purposes of Processing as specified in this Data Processing Agreement and the Services Agreement, and are intended to protect Personal Information against the risks inherent to the Processing of Personal Information in the performance of the Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored or otherwise Processed. Oracle Health may amend the TOMs as needed in order to protect Personal Information as specified in this Section 8. In this process, Oracle Health will consider in particular any technological progress. Changes to the TOMs may not lead to a reduced level of security.

8.2 You can view the current version of Oracle Health's Technical and Organizational Measures in the Oracle Health Data Protection Portal or request them from your support contact.

8.3 All Oracle Health and Oracle Affiliate staff, as well as any Third Party Subprocessors that Process Personal Information, are subject to a statutory confidentiality obligation or appropriate written data secrecy/ confidentiality arrangements in accordance with applicable laws, and have been duly instructed on the protective regulations of such laws. The undertaking of confidentiality shall continue after the termination of this Data Processing Agreement and the Service Agreement.

9. Audit Rights and Cooperation with You and Your Supervisory Authorities

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

9.2 In the course of such audit, and subject to the confidentiality terms of the Agreement, You may request Oracle Health to provide (i) available Service-related information and written documentation, and (ii) existing attestation or certificate by an independent professional expert.

9.3 If You determine that an additional audit is needed, such request shall be made to Oracle Health in writing. Oracle Health shall have an appropriate opportunity to respond to such request. After such exchange, insofar as You find on-site inspections to be necessary, the audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to Oracle Health'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 qualified, should not be an Oracle Health competitor, shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle Health. Upon completion of the audit, You will provide Oracle Health with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement.

9.4 Oracle Health 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,

Framework Ref: RM1557.15

Project Version: v1.1

Model Version: v1.0 PA

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle Health 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 Services Agreement.

9.5 You may also request that Oracle Health 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.

10. Incident Management and Personal Information Breach Notification

10.1 Oracle Health 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 Data (as such term is defined in the Services Agreement) that You provide transmitted, stored or otherwise Processed. Oracle Health 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.

10.2 Oracle Health 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 Health, Oracle Health 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 Health 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.

11. Return and Deletion of Personal Information

11.1 Upon termination of the Services, Oracle Health will promptly return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Information on Your Services production environment, except as otherwise stated in the Services Agreement.

11.2 For Services for which no data retrieval functionality is provided by Oracle Health 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.

12. Legal Requirements

12.1 Oracle Health 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.

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

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, which may include Applicable European Data Protection Law.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

“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; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended; and (iii) the UK Data Protection Act 2018, as amended.

“Data Subject”, “Process/Processing”, “Controller”, “Processor”, “Supervisory Authority” and “Binding Corporate Rules” (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

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

“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 data, including Personal Information, transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of Your data, including Personal Information.

“Oracle Health” means the Oracle Affiliate that has executed Services Agreement.

“Oracle Health and Oracle Affiliate(s)” means the subsidiar(y)(ies) of Oracle and Oracle Corporation that may Process Personal Information as set forth in Sections 2.2 and 7.

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

“Section” means a section of this Data Processing Agreement.

“Services” or the equivalent terms **“Service Offerings”** or **“services”** means the services specified in the Services Agreement.

“Services Agreement” means (i) the applicable order for the Services you have purchased from Oracle Health; (ii) the applicable master agreement referenced in the applicable order, and (iii) any applicable service specifications or descriptions.

“Third Party Subprocessor” means a third party, other than an Oracle Affiliate, which Oracle Health subcontracts with and which may Process Personal Information as set forth in Sections 2.2 and 7.

“You” means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement or as otherwise specified in this Data Processing Agreement.

Joint Schedule 10 (Processing Data)

1. Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (*Definitions*):

“Joint Control”	where two (2) or more Controllers jointly determine the purposes and means of Processing;
“Joint Controllers”	has the meaning given in Article 26 of the UK GDPR, or EU GDPR, as the context requires; and
“Processor Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract.

2. Status of the Controller

2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- 2.1.1 “Controller” in respect of the other Party who is “Processor”;
- 2.1.2 “Processor” in respect of the other Party who is “Controller”;
- 2.1.3 “Joint Controller” with the other Party;
- 2.1.4 “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

3. Where one Party is Controller and the other Party its Processor

3.1 Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller or further provided in writing by the Controller and may not be determined by the Processor.

3.2 The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.

3.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

- 3.3.1 a systematic description of the envisaged Processing and the purpose of the Processing;
- 3.3.2 an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
- 3.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and
- 3.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data; and
- 3.3.5 providing assurance that the measures referred to in Paragraph 3.3.4 comply with the Security Requirements (if any).

3.4 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- 3.4.1 process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) or as further provided in writing by the Controller, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;
- 3.4.2 ensure that it has in place Protective Measures including in the case of the Supplier the measures set out in this Joint Schedule 10 (*Processing Data*), Clause 17.3 of the General Terms and the Security Requirements (if any), which the Controller may reasonably reject (including, where applicable in accordance with its rights of rejection under those provisions) but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
 - (a) nature of the data to be protected;
 - (b) harm that might result from a Data Loss Event;
 - (c) state of technological development; and
 - (d) cost of implementing any measures.
- 3.4.3 ensure that:
 - (a) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*)) and the Controller's further written instructions;
 - (b) it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (i) are subject to any staff vetting required by this Contract, including the Security Requirements (if any);
 - (ii) are aware of and comply with the Processor's duties under this Joint Schedule 10, the Security Requirements (if any) and Clauses 17 (*Data protection*), 18 (*What you must keep confidential*) and 19 (*When you can share information*) of the General Terms;
 - (iii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (iv) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (v) have undergone adequate training in the use, care, protection and handling of Personal Data (including any training required by the Security Requirements (if any));
- 3.4.4 not transfer Personal Data outside of the UK and/or the EEA unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (a) the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74 of the DPA 2018) and/or Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:
 - (i) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

- (ii) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 3.4.4(a); and
- (iii) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):
 - (A) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 3.4.4(a);
 - (B) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 3.4.4(a); and/or
 - (C) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 3.4.4(a)(ii) above,

the Buyer shall have the right to terminate this Contract with immediate effect; or

- (b) the Controller and/or the Processor have provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:
 - (i) where the transfer is subject to UK GDPR;
 - (A) the International Data Transfer Agreement ("issued by the Information Commissioner under s119A(1) of the DPA 2018 (the **"IDTA"**)); or
 - (B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (**"EU SCCs"**) together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the **"Addendum"**), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018; and/or
 - (ii) where the transfer is subject to EU GDPR, the EU SCCs, as well as any additional measures being determined by the Controller being implemented by the importing party;
- (c) the Data Subject has enforceable rights and effective legal remedies;

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- (d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - 3.4.5 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 3.5 Subject to Paragraph 3.6 of this Joint Schedule 10, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
 - 3.5.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 3.5.2 receives a request to rectify, block or erase any Personal Data;
 - 3.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 3.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - 3.5.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - 3.5.6 becomes aware of a Data Loss Event.
- 3.6 The Processor's obligation to notify under Paragraph 3.5 of this Joint Schedule 10 shall include the provision of further information to the Controller, as details become available.
- 3.7 Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 3.5 of this Joint Schedule 10 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
 - 3.7.1 the Controller with full details and copies of the complaint, communication or request;
 - 3.7.2 such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - 3.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - 3.7.4 assistance as requested by the Controller following any Data Loss Event; and/or
 - 3.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.
- 3.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 10. This requirement does not apply where the Processor employs fewer than two hundred and fifty (250) staff, unless:
 - 3.8.1 the Controller determines that the Processing is not occasional;
 - 3.8.2 the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- 3.8.3 the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 3.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 3.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 3.11 Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - 3.11.1 notify the Controller in writing of the intended Subprocessor and Processing;
 - 3.11.2 obtain the written consent of the Controller;
 - 3.11.3 enter into a written agreement with the Subprocessor which gives effect to the terms set out in this Joint Schedule 10 such that they apply to the Subprocessor; and
 - 3.11.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 3.12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
- 3.13 The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 10 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
- 3.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office, any relevant Central Government Body and/or any other regulatory authority. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office, relevant Central Government Body and/or any other regulatory authority.

The terms set out in Paragraphs 3.15 to 3.21 below apply only to Contracts entered into under Lot 1a (*Infrastructure as a Service (IaaS)* and *Platform as a Service (PaaS)*) and Lot 1b (*Infrastructure as a Service (IaaS)* and *Platform as a Service (PaaS)*) above OFFICIAL

- 3.15 The Supplier warrants that the Subprocessors as at the Framework Start Date shall be those set out in the Supplier's Register of Key Subcontractors and Subprocessors as at that date. Throughout the Framework Contract Period and for the duration of all Call-Off Contracts the Supplier shall notify promptly CCS in writing of any additional or replacement Subprocessors appointed after the Framework Start Date in accordance with the provisions of Paragraph 3.17.
- 3.16 The Supplier shall maintain at all times throughout the Framework Contract Period an accurate, complete and up to date list of all Subprocessors used in the provision of the Services (the "**Supplier Register of Subprocessors**"), such list to contain as a minimum:
 - 3.16.1 the trading name of each Subprocessor and their respective registered company name, if different;
 - 3.16.2 a brief description of each Subprocessor's role in the provision of the Services;
 - 3.16.3 whether each Key Subcontractor should reasonably be categorised as a Subprocessor under Data Protection Legislation; and
 - 3.16.4 details of any third party which is not a Key Subcontractor but which should reasonably be categorised as a Subprocessor under Data Protection Legislation.
- 3.17 The Supplier shall give promptly notify CCS in writing of any additional or replacement Subprocessors appointed during the Framework Contract Period. Subject to Paragraph 3.18, it will not be necessary for the Supplier to obtain the prior consent of CCS to any additional or replacement Subprocessors. The Parties acknowledge and agree that such additional or replacement Subprocessors shall only apply to future Call-Off Contracts and not those already entered into between various Buyers and the Supplier.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- 3.18 If any proposed additional or replacement Subprocessor is an excluded or excludable supplier within the meaning of the Procurement Act 2023 and any associated Regulations, the proposed Subprocessor will only be approved for the purposes of Paragraph 3.11 of this Schedule if CCS gives its prior written consent.
- 3.19 The Supplier Register of Subprocessors is the Supplier's Confidential Information. For the avoidance of doubt, the Confidential Information that CCS may disclose under Clause 18.4 of the General Terms, including to Buyers or potential Buyer, shall include the Supplier Register of Key Subcontractors.
- 3.20 The relevant Controller provides general written consent to the Processor to engage those Subprocessors (including relevant details of such Subprocessor's processing of Personal Data) as recorded in the Supplier's Register of Subprocessors as at the Framework Start Date, provided that before allowing any Subprocessor to Process any Personal Data related to any Contract, the Processor must:
- 3.20.1 enter into a written agreement with the Subprocessor which gives effect to the terms set out in Paragraphs 3.1 to 3.14 of this Schedule such that they apply to the Subprocessor; and
 - 3.20.2 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 3.21 Where the Supplier intends to appoint a Subprocessor under a Call-Off Contract and that Subprocessor is not identified as a Subprocessor in the Supplier Register of Subprocessors or in the relevant Order Form, the Supplier shall provide not less than 30 (thirty) days' prior written notice via email to the Buyer Authorised Representative. Where the Buyer reasonably believes such proposed Subprocessor has, or is likely to have a materially adverse impact on:
- 3.21.1 the Buyer's use and enjoyment of the Services under the Contract;
 - 3.21.2 the commercial benefits of the Contract to the Buyer (including in relation to pricing and performance of the Services); and/or
 - 3.21.3 the balance of risks under the Contract from the Buyer's perspective (including the creation of new or increased potential liabilities and/or new or materially different operational responsibilities for the Buyer and/or any Buyer Users),
- the Buyer may, acting reasonably, object to such proposed appointment by notifying the Supplier in writing within 30 (thirty) days' of the Buyer's receipt of the Supplier's email notice of proposed appointment. If the Parties (acting reasonably) are unable within the next 10 (ten) days to resolve the Buyer's objection to its reasonable satisfaction the Buyer may terminate this Contract with immediate effect and without any liability (including, for the avoidance of doubt, pursuant to Clause 4.12 of the General Terms (that Clause 4.12 having been inserted in the General Terms pursuant to Framework Special Term 6 as set out in the Framework Award Form)) by giving notice in writing to the Supplier.

4. Where the Parties are Joint Controllers of Personal Data

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 (Joint Controllers Agreement) to this Joint Schedule 10.

5. Independent Controllers of Personal Data

- 5.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
- 5.2 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
- 5.3 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 5.2 of this Joint Schedule 10 above, the recipient of the Personal Data will

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

5.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

5.5 The Parties shall only provide Personal Data to each other:

5.5.1 to the extent necessary to perform their respective obligations under the Contract;

5.5.2 in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects:

(a) where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK and/or the EEA, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country (and if applicable the entity receiving the Personal Data) has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or Article 45 of the EU GDPR (where applicable), provided that if the destination country of a transfer is the United States:

(A) the Supplier shall ensure that prior to the transfer of any Personal Data to the United States relying on this adequacy (including to any United States-based Subcontractors and/or Subprocessors), the Supplier (and/or the applicable Subcontractor and/or Subprocessor) must be self-certified and continue to be self-certified on the US Data Privacy Framework;

(B) the Supplier shall notify the Buyer immediately if there are any, or there are reasonable grounds to believe there may be any, changes in respect of their and/or their Subcontractor's or Subprocessor's position on the US Data Privacy Framework (for example if that entity ceases to be certified or is at risk of being so, or there is a strong likelihood of a competent court finding the US Data Privacy Framework unlawful), and the Supplier must then take all appropriate steps to remedy the certification and/or put in place alternative data transfer mechanisms in compliance with this Paragraph 5.5.2(a)(i); and

(C) in the event that the Supplier (and/or the applicable Subcontractor or Subprocessor):

(1) ceases to be certified on the US Data Privacy Framework and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 5.5.2(a)(i);

(2) the US Data Privacy Framework is no longer available and the Supplier does not put in place the alternative data transfer mechanisms required for compliance with this Paragraph 5.5.2(a)(i); and/or

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- (3) fails to notify the Buyer of any changes to its certification status in accordance with Paragraph 5.5.2(a)(i)(B) above,
the Buyer shall have the right to terminate this Contract with immediate effect; or
- (b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable)) as determined by the non-transferring Party which could include:
 - (i) where the transfer is subject to UK GDPR:
 - (A) the International Data Transfer Agreement (the "**IDTA**") as published by the Information Commissioner's Office or such updated version of such IDTA as is published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time; or
 - (B) the European Commission's Standard Contractual Clauses per decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or
 - (ii) where the transfer is subject to EU GDPR, the EU SCCs, as well as any additional measures determined by the Controller being implemented by the importing party;
- (c) the Data Subject has enforceable rights and effective legal remedies;
- (d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and
- (e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

4.5.4 where it has recorded it in Annex 1 (*Processing Personal Data*).

- 5.6 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
- 5.7 A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
- 5.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("**Request Recipient**"):

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

- 5.8.1 the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
- 5.8.2 where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (a) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (b) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 5.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - 5.9.1 do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - 5.9.2 implement any measures necessary to restore the security of any compromised Personal Data;
 - 5.9.3 work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - 5.9.4 not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 5.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 5.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 5.12 Notwithstanding the general application of Paragraphs 3.1 to 3.14 of this Joint Schedule 10 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 5.2 to 5.12 of this Joint Schedule 10.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

Processing details for the Framework Contract

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: gdprgeneralenquiries@crowncommercial.gov.uk
- 1.2 The contact details of the Supplier's Data Protection Officer are as detailed in the Supplier Privacy Policy at <https://www.oracle.com/legal/privacy/>.
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor Not Applicable The Supplier is Controller and the Relevant Authority is Processor Not Applicable The Parties are Joint Controllers Not Applicable The Parties are Independent Controllers of Personal Data The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Relevant Authority and the Supplier are Independent Controllers of the following Personal Data: • Any Personal Data for effective communication between CCS and the Supplier. • Any Personal Data for maintaining full and accurate records of the Framework Contract.
Subject matter of the Processing	Not Applicable
Duration of the Processing	Not Applicable
Nature and purposes of the Processing	Not Applicable
Type of Personal Data	Not Applicable
Categories of Data Subject	Not Applicable

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	Not Applicable
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	Not Applicable
Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under the Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event (noting that any Protective Measures are to be in accordance with any Security Requirements)	Not Applicable

Processing details for the Call-Off Contract

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are as notified to Supplier from time to time in writing
- 1.2 The contact details of the Supplier's Data Protection Officer are as detailed in the Supplier Privacy Policy at <https://www.oracle.com/legal/privacy/>
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller in accordance with the Supplier Data Processing Agreement (as defined in the Supplier Terms at the start of this Order Form).
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • <i>Personal Information that Supplier processes on the Relevant Authority's behalf for the provision of the services.</i> The Supplier is Controller and the Relevant Authority is Processor

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with Paragraph 2 of the following Personal Data: • <i>Not applicable</i> The Parties are Joint Controllers The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: • <i>Not applicable</i> The Parties are Independent Controllers of Personal Data <i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i> • <i>Business contact details of Supplier Personnel for which the Supplier is the Controller,</i> • <i>Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller.</i>
Subject matter of the Processing	[Insert This should be a high level, short description of what the processing is about i.e. its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide [insert description of relevant service].]
Duration of the Processing	Supplier may Process Personal Information during the term of the Call-Off Contract and to perform its obligations relating to the return or deletion of such Personal Information, unless otherwise required by applicable law.
Nature and purposes of the Processing	[Insert Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	[Insert Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Insert Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	[Insert Describe how long the data will be retained for, how it be returned or destroyed]
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	In accordance with the Supplier Data Processing Agreement (as defined in the Supplier Terms at the start of this Order Form).

Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Crown Copyright 2025

Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under the Contract against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event (noting that any Protective Measures are to be in accordance with any Security Requirements)	The Supplier has Cyber Essentials Basic as a minimum baseline security control for the applicable Lot 2b Call-Off Contract.
---	---

Call-Off Schedule 20 (Call-Off Specification)

[Note: Order details to be provided by the Supplier to the Buyer prior to entering a Call-Off Contract]

This Schedule sets out the characteristics of the Deliverables and Supplier Service Descriptions that the Supplier will be required to make available to the Buyers under this Call-Off Contract. References in Schedule to “Oracle” “we”, “us”, or “our” are references to Oracle Corporation UK Limited and references to “Customer”, “You” or “Your” are to the Buyer identified in the Order Form. Any capitalised terms not defined below in this schedule shall have the meaning ascribed to them in the Supplier Licence Terms.

A. ADDITIONAL SUPPLIER LICENCE TERMS

1. Solution Descriptions – means the Solution Descriptions applicable to the Services ordered under Call-Off Schedule 20 (Call-Off Specification) of this Call-Off Contract and may be accessed at <http://www.oracle.com/contracts> on the Oracle Health tab.

2. [INSERT ADDITIONAL APPROVED DEAL SPECIFIC TERMS ACCORDINGLY]

B. DELIVERABLES

Services	Quantity	Reference	Term	Fees (£)
[Insert service names]	[Insert]	Exhibit [Insert] to Supplier Licence Terms	[Insert]	[Insert]
			Subtotal	[Insert]

Supplier Licence Terms

Oracle 'Supplier Licence Terms' for **[insert]** Services under CCS Framework Contract
RM1557.15

[Note: Supplier Licence Terms (to include Supplier security policies) to be provided by the Supplier to the Buyer prior to entering a Call-Off Contract]