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

**Order Form**

# CALL-OFF REFERENCE: 713050453

THE BUYER: DIO Ministry of Defence

BUYER ADDRESS Defence Infrastructure Organisation

Redacted

THE SUPPLIER: Redacted

SUPPLIER ADDRESS:Redacted

SUPPLIER CONTACT: Redacted

REGISTRATION NUMBER:

DUNS NUMBER: 738152433

SID4GOV ID:

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 6th February 2024.

It’s issued under the Framework Contract with the reference number Legal Services Panel RM6179 for the provision of legal advice and services.

CALL-OFF LOT(S):

**Lot 1 – General Legal Advice and Services**

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 and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6179
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

* Joint Schedules for RM6179
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data)
  + Joint Schedule 12 (Supply Chain Visibility)

* Call-Off Schedules for **713050453**
  + Call-Off Schedule 1 (Transparency Reports)
  + Call-Off Schedule 2 (Staff Transfer)
  + Call-Off Schedule 3 (Continuous Improvement)
  + Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  + Call-Off Schedule 12 (Clustering)
  + Call-Off Schedule 13 (Implementation Plan and Testing)
  + Call-Off Schedule 17 (MOD Terms)
  + Call-off Schedule 20 (Specification)
  + Call-Off Schedule 24 (Special Schedule)

1. CCS Core Terms (version 3.0.11)
2. Joint Schedule 5 (Corporate Social Responsibility)RM6179

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

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

None

CALL-OFF START DATE: **22nd October 2024**

CALL-OFF EXPIRY DATE: **5th February 2026**

CALL-OFF INITIAL PERIOD: 15 months

WORKING DAY

Monday to Friday 7 hours 24 minutes per day

CALL-OFF DELIVERABLES

The Buyer is entitled to 2 hours of free initial consultation and legal advice with each Order in accordance with Paragraph 5.2 of Framework Schedule 1 (Specification).

Deliverables

Redacted

MANAGEMENT OF CONFLICT OF INTEREST

None

CONFIDENTIALITY

None

IPR

None

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, and as amended by the Framework Special Terms.

CALL-OFF CHARGES

Total estimate of fees for remaining work to completion are £81,968.75.

All figures are exclusive of VAT and out of pocket disbursements are based on estimates of the time costs for each phase at the CCS rates charged to DIO rather than fixed fees.

Monthly invoices and timesheets for work completed will be submitted by the Supplier for review and approval by the MOD case officer before payment.

VOLUME DISCOUNTS

Where the Supplier provides Volume Discounts, the applicable percentage discount (set out in Table 2 of Annex 1 of Framework Schedule 3 (Framework Prices)) shall automatically be applied by the Supplier to all Charges it invoices regarding the Deliverables on and from the date and time when the applicable Volume Discount threshold is met and in accordance with Paragraphs 8, 9 and 10 of Framework Schedule 3.

REIMBURSABLE EXPENSES

None

DISBURSEMENTS

Out of pocket disbursements are paid in accordance with agreement with MOD case officer.

ADDITIONAL TRAINING CHARGE

None

SECONDMENT CHARGE

None

PAYMENT METHOD

Via CP&F

BUYER’S INVOICING ADDRESS:

Redacted

BUYER’S AUTHORISED REPRESENTATIVE

Redacted

BUYER’S ENVIRONMENTAL POLICY

https://[www.gov.uk/government/publications/jsp-418-mod-corporate-environmental-](http://www.gov.uk/government/publications/jsp-418-mod-corporate-environmental-) protection-manual

BUYER’S SECURITY POLICY

https://[www.gov.uk/government/publications/security-policy-framework](http://www.gov.uk/government/publications/security-policy-framework)

BUYER’S ICT POLICY

Not applicable

SUPPLIER’S AUTHORISED REPRESENTATIVE

Redacted

SUPPLIER’S CONTRACT MANAGER

Redacted

PROGRESS REPORT

See call-off schedule 20

PROGRESS REPORT FREQUENCY

See call-off schedule 20

PROGRESS MEETINGS AND PROGRESS MEETING FREQUENCY

See call-off schedule 20

KEY STAFF

Not applicable

KEY SUBCONTRACTOR(S)

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

Not applicable

|  |  |  |  |
| --- | --- | --- | --- |
| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
| Signature: | Redacted | Signature: | Redacted |
| Name: | Redacted | Name: | Redacted |
| Role: | Redacted | Role: | Redacted |
| Date: | 23rd October 2024 | Date: | 23rd October 2024 |

**Joint Schedule 11 (Processing Data)**

**Definitions**

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

|  |  |
| --- | --- |
| **“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; |

**Status of the Controller**

* 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:
     1. “Controller” in respect of the other Party who is “Processor”;
     2. “Processor” in respect of the other Party who is “Controller”;
     3. “Joint Controller” with the other Party;
     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.

**Where one Party is Controller and the other Party its Processor**

* 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.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
  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:
     1. a systematic description of the envisaged Processing and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
  4. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
     1. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
     2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
        1. nature of the data to be protected;
        2. harm that might result from a Personal Data Breach;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure that :
        1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
        2. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
           1. are aware of and comply with the Processor’s duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
           2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
           3. 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
           4. have undergone adequate training in the use, care, protection and handling of Personal Data;
     4. not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
        1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
        2. the Data Subject has enforceable rights and effective legal remedies;
        3. 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
        4. 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
     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.
  5. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
     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
     6. becomes aware of a Personal Data Breach.
  6. The Processor’s obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
  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 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
     1. the Controller with full details and copies of the complaint, communication or request;
     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. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
     4. assistance as requested by the Controller following any Personal Data Breach; and/or
     5. assistance as requested by the Controller with respect to any request from the Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.
  8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
     1. the Controller determines that the Processing is not occasional;
     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
     3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
  9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
  10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
  11. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
      1. notify the Controller in writing of the intended Subprocessor and Processing;
      2. obtain the written consent of the Controller;
      3. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
      4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
  12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
  13. The Relevant Authority may, at any time on not less than thirty (30) Working Days’ notice, revise this Joint Schedule 11 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).
  14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. 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.

**Where the Parties are Joint Controllers of Personal Data**

* 1. 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 to this Joint Schedule 11.

**Independent Controllers of Personal Data**

* 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.
  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.
  3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
  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. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Contract;
     2. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
     3. where it has recorded it in Annex 1 *(Processing Personal Data).*
  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.
  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.
  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”)**:
     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
     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:
        1. 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
        2. 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.
  9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. work with the other Party to make any required notifications to the Information Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
     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.
  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).*
  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)*.
  12. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 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 18 to 28 of this Joint Schedule 11.

## Annex 1 - Processing Personal Data

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

* + - 1. The contact details of the Relevant Authority’s Data Protection Officer are:

Ian Henderson

MDO DPO

Ground Floor, Zone D,

MOD Main Building,

Whitehall, London,

SW1A 2HB

Jani Artym

Chief Information Office   
St George’s House

Defence Infrastructure Organisation Head Office

DMS Whittington

Lichfield, Staffordshire

WS14 9PY

* + - 1. The contact details of the Supplier’s Data Protection Officer are: Edward Heath

[Edward.Heath@burges-salmon.com](mailto:Edward.Heath@burges-salmon.com)

* + - 1. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
      2. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 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:  *N/A*  **The Supplier is Controller and the Relevant Authority is Processor**  *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* 3 *to paragraph 16* *of the following Personal Data:*  N/A  **The Parties are Joint Controllers**  *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:*  *N/A*    **The Parties are Independent Controllers of Personal Data**  *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:*   * *Business contact details of Supplier Personnel for which the Supplier is the Controller,* * *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,* * Any personal data pertaining to Title Deeds, Leases, Rights or Covenants burdening the property or Restrictions on Disposition of Titles,the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the  Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority] |
| Duration of the Processing | *From contract award we would expect a Report within 2 weeks.*  *We expect all data to be deleted within two weeks of payment being made to the supplier.* |
| Nature and purposes of the Processing | *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 of the contract is the Evaluations of 175 Title Deeds.*  *Please refer to the Statement of Requirement, which outlines the data we require for processing along with our draft Report.* |
| Type of Personal Data | *Data that is found on the Titles, Business card personal data such names, addresses, telephone numbers, email address, images, telephone number, and roles. Any personal data pertaining to Title Deeds, Leases, Rights or Covenants burdening the property or Restrictions on Disposition of Titles.* |
| Categories of Data Subject | *Please refer to our draft Report which outlines the categories required*  *Staff business card personal data (Staff includes volunteers, agents, and temporary workers), users of secure shared areas.* |
| 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 | *The data will be retained for the duration of the contract. The supplier will apply the appropriate technical and organisational controls on the data to keep it safe and secure during the duration of the contract. The supplier is to securely destroy the data once the contract has ended and payment has been made.* |

**Annex 2 - Joint Controller Agreement**

**1. Joint Controller Status and Allocation of Responsibilities**

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Supplier/DIO on behalf of MOD:

* + 1. is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
    2. shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
    3. is solely responsible for the Parties’ compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
    4. is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
    5. shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier’s/Relevant Authority’s] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

* + 1. **Undertakings of both Parties**
       1. The Supplier and the Relevant Authority each undertake that they shall:
    2. report to the other Party every 8 weeks on:
       1. the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
       2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
       3. any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party’s obligations under applicable Data Protection Legislation;
       4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
       5. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

* + 1. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
    2. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
    3. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
    4. request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
    5. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
    6. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
       1. are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
       2. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
       3. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
    7. ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
       1. nature of the data to be protected;
       2. harm that might result from a Personal Data Breach;
       3. state of technological development; and
       4. cost of implementing any measures;
    8. ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
    9. ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.
       1. Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.
    10. **Data Protection Breach**
        1. Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
    11. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
    12. all reasonable assistance, including:
        1. co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
        2. co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
        3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
        4. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.
        5. Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party’s own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:
    13. the nature of the Personal Data Breach;
    14. the nature of Personal Data affected;
    15. the categories and number of Data Subjects concerned;
    16. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
    17. measures taken or proposed to be taken to address the Personal Data Breach; and
    18. describe the likely consequences of the Personal Data Breach.
    19. **Audit**
        1. The Supplier shall permit:
    20. the Relevant Authority, or a third-party auditor acting under the Relevant Authority’s direction, to conduct, at the Relevant Authority’s cost, data privacy and security audits, assessments and inspections concerning the Supplier’s data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
    21. the Relevant Authority, or a third-party auditor acting under the Relevant Authority’s direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.
        1. The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier’s compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.
    22. **Impact Assessments**
        1. The Parties shall:
    23. provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
    24. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.
    25. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. 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 and/or any relevant Central Government Body.

* + 1. **Liabilities for Data Protection Breach**
       1. If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:
    2. if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
    3. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
    4. if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).
       1. If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
       2. In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):
    5. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
    6. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
    7. if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.
       1. Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.
    8. **Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

* + 1. **Sub-Processing**
       1. In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
    2. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
    3. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.
    4. **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

**Call-Off Schedule 17 (MOD Terms)**

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

|  |  |
| --- | --- |
| **"MOD Terms and Conditions"** | the terms and conditions listed in this Schedule; |
| **"MOD Site"** | shall include any of Her Majesty's Ships or Vessels and Service Stations; |
| **"Officer in charge"** | shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments; |

1. **Access to MOD sites**
   1. The Buyer shall issue passes for those representatives of the Supplier who are approved for admission to the MOD Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Buyer and shall be surrendered on demand or on completion of the supply of the Deliverables.
   2. The Supplier's representatives when employed within the boundaries of a MOD Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of staff at that MOD Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.
   3. The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a MOD Site. Sleeping accommodation and messing facilities, if required, may be provided by the Buyer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At MOD Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's staff for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his decision before the commencement of this Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Buyer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Buyer with other evidence relating to the costs of this Contract.
   4. Where the Supplier's representatives are required by this Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in the Buyer Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Buyer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is necessary for the purpose of this Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.
   5. Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.
   6. Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc. Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.
   7. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.
   8. The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Buyer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Supplier's representatives are attached. All such advances made by the Buyer shall be recovered from the Supplier

# DEFCONS and DEFFORMS

## The DEFCONS and DEFORMS listed in Annex 1 to this Schedule are incorporated into this Contract.

## Where a DEFCON or DEFORM is updated or replaced the reference shall be taken as referring to the updated or replacement DEFCON or DEFORM from time to time.

## In the event of a conflict between any DEFCONs and DEFFORMS listed in the Order Form and the other terms in a Call Off Contract, the DEFCONs and DEFFORMS shall prevail.

# Authorisation by the Crown for use of third party intellectual property rights

## Notwithstanding any other provisions of the Call Off Contract and for the avoidance of doubt, award of the Call Off Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any such authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

**ANNEX 1 - DEFCONS & DEFFORMS**

The full text of Defence Conditions (DEFCONs) and Defence Forms (DEFFORMS) are available electronically via <https://www.gov.uk/guidance/knowledge-in-defence-kid>.

The following MOD DEFCONs and DEFFORMs form part of this contract:

DEFCONs

|  |  |  |
| --- | --- | --- |
| **DEFCON No** | **Version** | **Description** |
| **5J** | EDN 11/16 | Unique Identifiers |
| **76** | EDN 06/21 | Contractors’ Personnel at Government Establishments |
| **501** | EDN 10/21 | Definitions And Interpretations |
| **503** | EDN 07/21 | Formal Amendment to Contract |
| **513** | EDN 04/22 | Value Added Tax |
| **514** | EDN 08/15 | Material Breach |
| **515** | EDN 06/21 | Bankruptcy And Insolvency |
| **516** | EDN 04/21 | Equality |
| **518** | EDN 02/17 | Transfer |
| **520** | EDN 08/21 | Corrupt Gifts and Payment of Commission |
| **522** | EDN 11/21 | Payment and Recovery of Sums Due |
| **529** | EDN 09/97 | LAW ( English) |
| **530** | EDN 09/21 | Dispute Resolution (English Law |
| **531** | EDN 09/21 | Disclosure of Information |
| **532B** | EDN 09/21 | Protection of Personal Data |
| **534** | EDN 06/21 | Subcontracting And Prompt Payment |
| **537** | EDN 12/21 | Rights of Third Parties |
| **538** | EDN 06/02 | Severability |
| **539** | EDN 08/13 | Transparency |
| **550** | EDN 02/14 | Child labour and Employment Law |
| **566** | EDN 10/20 | Change Of Control Of Contractor |
| **602B** | EDN 12/06 | Quality Assurance (Without Quality Plan) |
| **604** | EDN 06/14 | Progress Reports |
| **642** | EDN 07/21 | Progress meetings (1 PAGE) |
| **649** | EDN 12/21 | Vesting |
| **656A** | EDN 08/16 | Termination for Convenience – Under £5M |
| **658** | EDN 09/21 | Cyber (Cyber Risk Profile for the contract |
| **659A** | EDN 12/15 | Security Measures |
| **660** | EDN 12/15 | Official-Sensitive Security Requirements |
| **670** | EDN 02/17 | Tax Compliance |
| **703** | EDN 06/21 | Intellectual Property rights – vesting in the authority |

DEFFORMs (Ministry of Defence Forms)

|  |  |  |
| --- | --- | --- |
| **DEFFORM No** | **Version** | **Description** |
| **532** | **EDN 10/19** | **Personal Data Particulars** |

**Call-Off Schedule 20 (Call-Off Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Redacted

Monthly invoices and timesheets for work will be submitted for review and approval by the MOD case officer.