

## G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

### **G-Cloud 13 Call-Off Contract**

Part A: Order Form

2

Part B: Terms and conditions

15

Schedule 1: Services

36

Schedule 2: Call-Off Contract charges

37

Schedule 3: Collaboration agreement

38

Schedule 4: Alternative clauses

51

Schedule 5: Guarantee

56

Schedule 6: Glossary and interpretations

65

Schedule 7: UK GDPR Information

83

Annex 1: Processing Personal Data

84

Schedule 8: Statement of Works Template

95

## Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

<b>Platform service ID number</b>	7518 9870 2122 764
<b>Call-Off Contract reference</b>	Document Handling and Transcription Services
<b>Call-Off Contract title</b>	TMAR3112
<b>Call-Off Contract description</b>	This Call Off Contract shall enable DfT's Cranston Inquiry Team to procure Opus 2 Documents Handling and Transcriptions services for inquiries and other legal hearings. They will bundle documents taken from Relativity and prepare them for electronic presentation in Inquiry hearings. They will also provide a live transcript of the Hearings.
<b>Start date</b>	09 <sup>th</sup> May 2024
<b>Expiry date</b>	08 <sup>th</sup> May 2025
<b>Call-Off Contract value</b>	Up to £300,000 with an initial commitment to spend £171,520 exc VAT.
<b>Charging method</b>	BACS

<b>Purchase order number</b>	TBC
------------------------------	-----

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

<b>From the Buyer</b>	Department for Transport Great Minster House 33 Horseferry Road Westminster London SW1P 4DR
<b>To the Supplier</b>	OPUS 2 INTERNATIONAL LIMITED 5th Floor (C/O Opus 2) 5 New Street Square London England EC4A 3BF Company number: 05907841

**Together the 'Parties'**

Principal contact details

**For the Buyer:**

Title: Head of Operations and Delivery

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

**For the Supplier:**

Title: Senior Business Development Associate

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on 09 <sup>th</sup> May 2024 and is valid for 12 months.
-------------------	--

<b>Ending (termination)</b>	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
<b>Extension period</b>	<p>This Call-Off Contract can be extended by the Buyer for <b>one</b> period of up to 12 months, by giving the Supplier one month's written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p><a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a></p>

### Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

<b>G-Cloud Lot</b>	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> <li>• Lot 2: Cloud Software</li> </ul>
<b>G-Cloud Services required</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined</p>

	within the Suppliers Service Offering: 7518 9870 2122 764.
<b>Additional Terms</b>	<p>The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template) set out in Schedule 8 of this Call Off Order Form.</p> <p>Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.</p> <p>The Parties agree that the price for the Services provided under this Call-Off Contract may be subject to re-negotiation. The Buyer or the Supplier may initiate a price re-negotiation by providing written notice to the other Party. The Parties shall negotiate in good faith to reach a mutually acceptable revised price. If the Parties are unable to reach an agreement on the revised price within 30 days of the initiation of the re-negotiation, the Contract shall continue under the original pricing terms. Any agreed-upon revised price shall be effective from the date specified in writing by the Parties.</p>
<b>Additional Services</b>	Additional services outlined in the Supplier Service Offering may be called off during the contract life.
<b>Location</b>	The Services will be delivered at the buyer's selected locations or remotely where appropriate.
<b>Quality Standards</b>	The quality standards required for this Call-Off Contract are contained with the Suppliers Service Offering: 7518 9870 2122 764
<b>Technical Standards:</b>	The technical standards used as a requirement for this Call-Off Contract are outlined within the Suppliers Service Offering: 7518 9870 2122 764.
<b>Service level agreement:</b>	The service level and availability criteria required for this Call-Off Contract is outlined within the Suppliers Service Offering: 7518 9870 2122 764.

<b>Onboarding</b>	Online or onsite training provided as required. User guide provided to all users upon access to the platform. Ongoing phone and email support and further training where required by the users.
<b>Offboarding</b>	Offline PDF export to encrypted USB or secure file transfer site. Work product across the data set can also be extracted (by the user). Solution Operations Manager assigned to the case will provide post-instruction options to the Buyer; deletion, archiving, export and will provide an explanation, implications and costings for each option.
<b>Limit on Parties' liability</b>	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £1,000,000 per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<b>Insurance</b>	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>• professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim (and as required by Law).</li> <li>• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law</li> </ul>

<b>Buyer's responsibilities</b>	The Buyer will provide any necessary support or access for the supplier to deliver the required service. Before work commences, the buyer will agree with the supplier what, if any equipment is necessary.
<b>Buyer's equipment</b>	The Buyer will provide any necessary equipment for the supplier to deliver the necessary service. Before work commences, the buyer will agree with the supplier what, if any equipment is necessary.

#### Supplier's information

<b>Subcontractors or partners</b>	N/A
<b>Sub processors</b>	As per the terms within the Suppliers Service Offering: 7518 9870 2122 764.

#### Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.



<b>Payment method</b>	The payment method for this Call-Off Contract is BACS.
<b>Payment profile</b>	The payment profile for this Call-Off Contract is monthly in arrears.
<b>Invoice details</b>	The Supplier will issue electronic invoices once a quote has been agreed and completed to the standard required. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
<b>Who and where to send invoices to</b>	<p>Invoices will be sent to:</p> <p>Shared Services Arvato 5 Sandringham Park Swansea Vale Swansea SA7 0EA</p> <p>Alternatively, electronic Invoices can be issued to:</p> <p><a href="mailto:ssa.invoice@sharedservicesarvato.co.uk">ssa.invoice@sharedservicesarvato.co.uk</a></p>
<b>Invoice information required</b>	<p>The Supplier will issue electronic invoices and the Buyer will pay the Supplier within 30 days of receipt of a valid invoice.</p> <p>The invoice must include the PO number.</p>

<b>Invoice frequency</b>	Invoice will be sent to the Buyer Monthly.
<b>Call-Off Contract value</b>	The total value of this Call-Off Contract is up to £300,000 with a commitment to spend £171,520. DfT are not contractually obligated to use the full amount allocated to this Call-Off Contract.
<b>Call-Off Contract charges</b>	<p>The breakdown of the Charges will be included and agreed by both Parties (see Schedule 2 Call-Off Contract Charges).</p> <p>Supplier expenses shall be paid in accordance with DfT's Travel and Subsistence rates.</p>

#### Additional Buyer terms

<b>Performance of the Service</b>	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <p>Before any services are carried out, there must be an agreement between the Buyer and Supplier in terms of what is expected of the supplier in terms of performance and deliverables, which shall be set out using the Statement of Works template in Schedule 8.</p> <p>To identify performance and deliverables, the buyer should review the suppliers service levels and response times provided under Schedule 1 and consider setting milestones with associated Deliverables and agreeing payments against those Deliverables, as per the statement of work template in Schedule 8.</p> <p>The Buyer shall also consider including an Implementation Plan, exit and offboarding plans and milestones. An Exit Plan shall be provided by the Supplier within 6 months of contract start and be updated and reviewed with Buyer at a minimum every 6 months throughout the contract term.</p>
-----------------------------------	--

<b>Guarantee</b>	Not required.
<b>Personal Data and Data Subjects</b>	Annex 1 of Schedule 7 is being used.
<b>Intellectual Property</b>	No additional IPR clauses are required.
<b>Social Value</b>	The suppliers social value commitments are outlined within the Suppliers Service Offering: 7518 9870 2122 764.




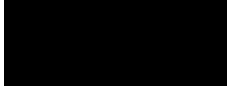
## 1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.
- 1.5 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

## 2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

2.2 The Buyer provided an Order Form for Services to the Supplier.

<b>Signed</b>	Supplier	Buyer
<b>Name</b>		
<b>Title</b>	Chief Commercial Officer	Procurement Business Partner
<b>Signature</b>		
<b>Date</b>	07/05/2024	[Enter date] 07/05/2024

## Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

[G-Cloud 13 Customer Benefit Record](#)

## Part B: Terms and conditions

### 1. Call-Off Contract Start date and length

- Form.
- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

### 2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
- 2.3 (Warranties and representations)
  - 4.1 to 4.6 (Liability)
  - 4.10 to 4.11 (IR35)
  - 10 (Force majeure)
  - 5.3 (Continuing rights)
  - 5.4 to 5.6 (Change of control)
  - 5.7 (Fraud)
  - 5.8 (Notice of fraud)
  - 7 (Transparency and Audit)
  - 8.3 (Order of precedence)
  - 11 (Relationship)
  - 14 (Entire agreement)
  - 15 (Law and jurisdiction)
  - 16 (Legislative change)
  - 17 (Bribery and corruption)
  - 18 (Freedom of Information Act)
  - 19 (Promoting tax compliance)

- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- 2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- 2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
- 2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract
- 2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.
- 2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.
- 2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

#### 4. Supplier staff

##### 4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.



## 5. Due diligence

### 5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

## 6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

## 7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

Rate.

- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoices under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

## 8. Recovery of sums due and right of set-off

- 8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

## 9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:

- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
  - 9.4.1 a broker's verification of insurance
  - 9.4.2 receipts for the insurance premium
  - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
  - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
  - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
  - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
- 9.8.1 premiums, which it will pay promptly
  - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

## 10. Confidentiality

- 10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither
- Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:
- 11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
- (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
- (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

- 11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - 11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.8 Clause 11.6 will not apply if the IPR Claim is from:
  - 11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.8.2 other material provided by the Buyer necessary for the Services
- 11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12. Protection of information

- 12.1 The Supplier must:
  - 12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
  - 12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
  - 12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes
- 12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
  - 12.2.1 providing the Buyer with full details of the complaint or request
  - 12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
  - 12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
  - 12.2.4 providing the Buyer with any information requested by the Data Subject

- 12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

### 13. Buyer data

- 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
- 13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
- 13.6.1 the principles in the Security Policy Framework:  
<https://www.gov.uk/government/publications/security-policy-framework>  
and the Government Security Classification policy:  
<https://www.gov.uk/government/publications/government-securityclassifications>
- 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:  
<https://www.cpni.gov.uk/content/adopt-risk-managementapproach>  
and Protection of Sensitive Information and Assets:  
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
- 13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>
- 13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:  
<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

- 13.7 The Buyer will specify any security requirements for this project in the Order Form.
- 13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## 14. Standards and quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:  
<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the

PSN

Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.



## 15. Open source

- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
- 15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

## 16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
  - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
  - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:  
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

## 17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

## 18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the

Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

- 18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

## 19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

## 20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

## 21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
  - 21.6.2 there will be no adverse impact on service continuity
  - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
  - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
  - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
  - 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
  - 21.8.4 the testing and assurance strategy for exported Buyer Data
  - 21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

## 22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

## 23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

## 24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6,

the

Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited;  
and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation  
shall be as set out in Framework Agreement clause 28.

the 24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6,

Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate  
five million pounds (£5,000,000).

Clause 24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in  
24.2 will not be taken into consideration.

## 25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or  
damage it causes to the premises. It is responsible for repairing any damage to the  
premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its  
obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or  
expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything  
to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes  
any damage to Property which could cause personal injury



- 25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

## 26. Equipment

- 26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.
- 26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

## 27. The Contracts (Rights of Third Parties) Act 1999

- 27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

## 28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

## 29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to

End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29.2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.5 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.5.1 its failure to comply with the provisions of this clause

29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise

from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

### 30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

### 31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

### 32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

### 33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

## Schedule 1: Services

The services carried out as per the Supplier Service Description and Service Offering 7518 9870 2122 764.

Work will be commissioned via Statements of Work (See Schedule 8).

## Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract.

The Suppliers rate card for the duration of this contract (including extensions options) is shown below:

# Pricing - Opus 2 Hearings Solution

## 1. Opus 2 Software

Workspace Preparation		Cost (excl VAT)
<b>Initial Document Upload</b>	Document uploads: <ul style="list-style-type: none"> <li>██</li> </ul>	████████
<b>Hyperlinking</b>	Hearing Bundle hyperlinks to cross referenced documents: <ul style="list-style-type: none"> <li>██</li> </ul> <i>*Manual hyperlinking is available upon request at a charge of ██████████</i>	TBC if required
<b>OCR'ing</b>	Running optical character recognition (OCR) over PDF documents to highlight, annotate and search. <ul style="list-style-type: none"> <li>██</li> </ul>	TBC if required
<b>Additional workspaces</b>	Creation of additional mirror workspaces (5 provided free of charge): <ul style="list-style-type: none"> <li>██</li> </ul>	TBC if required
<b>Content Management</b>	In the event that additional work is required after the initial ingestion and creation of the inquiry workspace, an hourly content management fee will be charged for tasks such as (but not limited to) structuring, metadata application, application of any access control lists (ACL), additions, replacements, inserts, re-ordering of documents, repurposing, re-structuring of folders, and sequential pagination: <ul style="list-style-type: none"> <li>██</li> </ul>	TBC if required
<b>Project Management</b>	Dedicated Project Manager to advise on workflows specific to the inquiry and provide best practice guidance across the project as a whole: <ul style="list-style-type: none"> <li>██</li> </ul>	TBC if required
<b>Training</b>	Training during standard business hours (9.00am to 6.00pm, Monday to Friday): <ul style="list-style-type: none"> <li>██</li> </ul> <i>Any travel fares and expenses - charged at cost.</i>	TBC if required
<b>Access Fees</b>	Opus 2 Software subscription - the tier selected at the outset will be applicable for the duration of the instruction and will form the basis on which user access fees are charged - 40 users for 6 months: <ul style="list-style-type: none"> <li>████████ per month for up to 25 users (additional users above 25 charged at ██████████ per user per month) or;</li> <li>████████ per month for up to 50 users (additional users above 50 charged at ██████████ per user per month) or;</li> <li>████████ per month for up to 100 users (additional users above 100 charged at ██████████ per user per month) or;</li> <li>████████ per month for up to 200 users (additional users above 200 charged at ██████████ per user per month) or;</li> <li>████████ per month for up to 300 users (additional users above 300 charged at ██████████ per user per month).</li> </ul> <i>Access fees are payable from when Opus 2 first grants access to users.</i>	████████

<b>Exporting/ Archiving</b>	<p>Encrypted USB containing an export of contents of workspace or electronic archive of workspace, preserving it in its existing form, for a period of 2 years. *</p> <p><i>*Based on number of documents.</i></p>	<b>TBC if required</b>
---------------------------------	--	------------------------

*Work conducted out of standard business working hours, charged at 1.5x applicable rate.*

Opus 2 Software cancellation		Cost (excl VAT)
<b>Software Fees</b>	All Opus 2 Software Services fees incurred up to the date of cancellation but not yet invoiced will be charged accordingly.	<b>Opus 2 Software fees incurred up until point of cancellation</b>



## 2. Opus 2 Hearing Services

Reporting team attendance		Cost (excl VAT)
<b>Attendance Fee</b>	Provision of a reporting team for up to 5.5 Sitting Hours: <ul style="list-style-type: none"> <li>■ [REDACTED] per Sitting Day for 24 days.</li> </ul>	[REDACTED]
<b>Overtime / extended days</b>	Additional Sitting Hours: <ul style="list-style-type: none"> <li>■ [REDACTED] per half hour.</li> </ul> <p><i>If the Sitting Hours meet or exceed 8 hours, two Attendance Fees will be charged in place of overtime. Please advise us if overtime is likely to ensure the allocation of an appropriate Reporting Team.</i></p>	TBC if required
Realtime and ancillary transcription services		Cost (excl VAT)
<b>Realtime Connections</b>	Realtime Connections inclusive of integrated private chat functionality and a complimentary laptop in the hearing room – 40 connections for 24 days: <ul style="list-style-type: none"> <li>■ [REDACTED] per connection, per day for the first 1 to 25 connections;</li> <li>■ [REDACTED] per connection, per day for the next 26-50 connections;</li> <li>■ [REDACTED] per connection, per day for any additional connections over 50.</li> </ul>	[REDACTED]
<b>First draft transcript</b>	Email in Word format as required during the lunch break for distribution and publication to the inquiry website: <ul style="list-style-type: none"> <li>■ [REDACTED] per day.</li> </ul>	TBC if required
<b>Evidence publishing</b>	Preparation and provision of referenced evidence to Inquiry Team on a daily basis for the purposes of publishing to the inquiry website: <ul style="list-style-type: none"> <li>■ Tier 1 - Opus 2 generate a list of referenced evidence based on the daily transcript and provide an export to the Inquiry Team - [REDACTED] per day or;</li> <li>■ Tier 2 - Opus 2 generate a list of referenced evidence split by witness / expert based on the EPE Officer's records and the daily transcript and provide an export to the Inquiry Team - [REDACTED] per day or;</li> <li>■ Tier 3 - as per Tier 2 above, and to include additional steps (in consultation with Inquiry Team) such as uploading export to the inquiry website (holding area) - [REDACTED] per day.</li> </ul>	TBC if required
Electronic Presentation of Evidence (EPE) Services		Cost (excl VAT)
<b>EPE operator</b>	Provision of an EPE operator, inclusive of 10 evidence display screens: <ul style="list-style-type: none"> <li>■ [REDACTED] per Sitting Day for 24 days.</li> </ul>	[REDACTED]
<b>EPE set-up</b>	EPE set-up, configuration and testing: <ul style="list-style-type: none"> <li>■ [REDACTED] per set-up.</li> </ul> <p><i>Chargeable 2 weeks in advance of the hearing.</i></p>	[REDACTED]
Technical Services		Cost (excl VAT)
<b>Technical Support</b>	Consultation for hearing room set-up and configuration, liaising and running test sessions with AV providers and advising on specific workflows for in-hearing services as required. <ul style="list-style-type: none"> <li>■ [REDACTED] per hour.</li> </ul>	TBC if required

Hearing server		Cost (excl VAT)
<b>Hearing Server set-up</b>	Preparation and configuration of the hearing server facilitating the integrated Realtime transcript and EPE enabling a fully hyperlinked transcript and live access to evidence: <ul style="list-style-type: none"> <li>■ [REDACTED]</li> </ul>	[REDACTED]
Virtual Hearing Services		Cost (excl VAT)
<b>Virtual Hearing set-up</b>	Configuration of the video conference for the Virtual Hearing to cover all pre-hearing technical consultancy, testing, and liaison with the Inquiry Team, including co-ordinating the protocol for the hearing and remote assistance for individual set-ups: <ul style="list-style-type: none"> <li>■ [REDACTED] per set-up.</li> </ul> <i>Chargeable 2 weeks in advance of the hearing.</i>	TBC if required
<b>Virtual Hearing access</b>	Access to the Virtual Hearing via audio or video conference, joining all participants to the hearing (and for litigation, facilitating a live stream of the proceedings in accordance with public access requirements): <ul style="list-style-type: none"> <li>■ [REDACTED] per Sitting Day for 1-10 participants;</li> <li>■ [REDACTED] per Sitting Day for 11-20 participants;</li> <li>■ [REDACTED] per Sitting Day for 21+ participants.</li> </ul>	TBC if required
<b>Virtual Hearing Manager</b>	Provision of a dedicated Virtual Hearing Manager to ensure the seamless delivery of the virtual hearing. Your Virtual Hearing Manager will act as the interface between the participants and the technology and services underpinning the virtual hearing, including constant monitoring and fault recovery for the duration of proceedings: <ul style="list-style-type: none"> <li>■ [REDACTED] per Sitting Day.</li> </ul>	TBC if required
<b>Virtual Hearing hardware packs</b>	Rental of key equipment for individual remote active participants including VOIP headset/personal speakerphone, 1080p camera and extended screen: <ul style="list-style-type: none"> <li>■ [REDACTED] per pack per Business Day.</li> </ul> <i>Rental fee incurred from day 1 of the hearing to the date the equipment is collected for return to Opus 2. Courier fees and any ancillary expenses charged at cost. Provision of equipment pack is subject to equipment availability and logistical considerations upon formal instruction and will be discussed at the time.</i>	TBC if required
<b>Managed audio / video feed for hybrid hearings</b>	Provision of high-spec audio-visual and video production equipment in the hearing room and a specialist on-site AV engineer to produce the video feed throughout the hearing: <ul style="list-style-type: none"> <li>■ [REDACTED] per Sitting Day.</li> </ul>	TBC if required
<b>AV set-up</b>	Configuration and set-up of the audio-visual and video production equipment: <ul style="list-style-type: none"> <li>■ [REDACTED] per set-up.</li> </ul> <i>Chargeable 2 weeks in advance of the hearing.</i>	TBC if required
Please advise us as soon as possible if the hearing may be virtual or hybrid (partly heard in-person, partly heard virtually with participants based remotely) so Opus 2 can best advise as to the delivery of hearing services, and any associated costs.		
Equipment carriage		Cost (excl VAT)
<b>Equipment carriage fees</b>	Delivery of equipment and collection at the conclusion of proceedings: <ul style="list-style-type: none"> <li>■ [REDACTED]</li> </ul>	[REDACTED]

Hearing Services Cancellation		Cost (excl VAT)
<b>Transcription Services</b>	Cancellation of Transcription Services on any individual Sitting Day (pre (including any floating window days) or post commencement of the hearing) after 10:00am on the preceding Business Day.	■
<b>EPE Services</b>	Cancellation of EPE Services on any individual Sitting Day (pre (including any floating window days) or post commencement of the hearing) after 10:00am on the preceding Business Day.	■

*If the Buyer is to instruct Opus 2 under the Framework as part of a multi-party case, then certain fees may be split to account for this, and the relevant proportion charged accordingly.*

## Additional benefits

What's included free of charge	
<b>Data hosting</b>	Storage of documents on a private server hosted in the UK.
<b>Transcript Hyperlinks</b>	Fully hyperlinked transcript to referenced documents.
<b>Electronic transcripts</b>	Final version of the transcript in ASCII, Word and Adobe Acrobat PDF (condensed with word index) circulated as standard at the end of each day.
<b>Synchronised audio</b>	Audio synchronised to the transcript at the end of the day, subject to the consent of all parties and permission from the Judge / Tribunal.
<b>Case management</b>	Your matter will be handled by a dedicated Case Manager. Our case managers are highly experienced in facilitating complex multi-party instructions and will work closely with all parties to ensure the successful delivery of the hearing in accordance with your requirements.



### 3. Service Enhancements (available upon request)

Service		Cost (excl VAT)
<b>Laptop or Tablet</b>	Additional pre-configured laptops or tablets to use during proceedings, to be connected to the hearing server in the venue to ensure a robust connection and avoid dependence on unreliable Wi-Fi or 3G. <ul style="list-style-type: none"> <li>■ per laptop per day.</li> <li>■ per tablet per day.</li> </ul>	TBC if required
<b>EPE Screens</b>	Additional evidence presentation screens: <ul style="list-style-type: none"> <li>■ per screen per day.</li> </ul>	TBC if required
<b>Large Format Display</b>	Certain documents, such as spreadsheets and construction drawings can be problematic to display on small screens. Opus 2 can provide large monitors to present these documents clearly: <ul style="list-style-type: none"> <li>■ per 46" screen per day or;</li> <li>■ per 65" screen per day.</li> </ul>	TBC if required
<b>Remote EPE</b>	Opus 2 can also connect off-site participants to the evidence being displayed during proceedings: <ul style="list-style-type: none"> <li>■ per remote participant per day.</li> </ul> <i>Applicable only to fully in-person hearings.</i>	TBC if required
<b>Live Audio Feed</b>	With the permission of the inquiry, we can provide a live audio feed of the hearing to off-site participants: <ul style="list-style-type: none"> <li>■ per feed per day.</li> </ul>	TBC if required
<b>Delay Stream Technology</b>	Implementation of delay to audio/visual feeds: <ul style="list-style-type: none"> <li>■ per day.</li> </ul>	TBC if required
<b>Hearing Audio</b>	Opus 2 can also provide a standalone audio file of the hearing. <ul style="list-style-type: none"> <li>■ per audio file provided by SFTP per day.</li> <li>■ per audio file provided by encrypted USB per day.</li> </ul>	TBC if required
<b>Site Visit</b>	Site attendance to assess the hearing venue and plan set-up: <ul style="list-style-type: none"> <li>■ per site visit.</li> </ul>	TBC if required
<b>Interpretation</b>	Set-up of any required equipment: <ul style="list-style-type: none"> <li>■ per set-up.</li> </ul>	TBC if required
	Provision of interpretation booth, service engineer, microphones, and headsets to facilitate simultaneous interpretation: <ul style="list-style-type: none"> <li>■ per day.</li> </ul>	TBC if required
<b>Speakers</b>	A set of two speakers: <ul style="list-style-type: none"> <li>■ per set per week.</li> </ul>	TBC if required
<b>Pointing devices</b>	Rental of device used to identify and draw reference to a particular area on a display screen: <ul style="list-style-type: none"> <li>■ per unit per day.</li> </ul>	TBC if required

*Subsistence, accommodation, travel fees and any other expenses for hearings outside of London to be agreed on a case-by-case basis.*

## Schedule 3: Collaboration agreement

Not required.

## Schedule 4: Alternative clauses

### 1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

### 2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative

Clauses: 2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework

Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

### 2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002

- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004 • Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

## **2.4 Equality policies and practices**

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The

Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities
- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

- A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations



similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

## **2.5 Equality**

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

## **2.6 Health and safety**

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

## **2.7 Criminal damage**

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

## Schedule 5: Guarantee

There's a guarantee of the Supplier's performance provided for all Call-Off Contracts entered under the Framework Contract.

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses.

<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.
<b>Buyer Software</b>	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.

<b>Call-Off Contract</b>	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
<b>Call-Off Contract Period</b>	the Contract Period in respect of the Call-Off Contract;
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

<b>Confidential Information</b>	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> <li>• information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the UK GDPR.
<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b>	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
<b>Data Protection Legislation (DPL)</b>	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
<b>Data Subject</b>	Takes the meaning given in the UK GDPR
<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>Deliverables</b>	Goods and/or Services that may be ordered under the Contract including the documentation;
<b>DPA 2018</b>	Data Protection Act 2018.



<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="https://www.gov.uk/guidance/check-employment-status-fortax">https://www.gov.uk/guidance/check-employment-status-fortax</a>

<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Force Majeure</b>	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>• the event was foreseeable by the Party seeking to rely on Force</li> </ul> <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> <li>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<b>Former Supplier</b>	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).

<b>Framework Agreement</b>	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
<b>Fraud</b>	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or

	defrauding or attempting to defraud or conspiring to defraud the Crown.
<b>Freedom of Information Act or FoIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
<b>UK GDPR</b>	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).

<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.

<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

<b>Insolvency event</b>	<p>Can be:</p> <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> <li>• a Dun &amp; Bradstreet rating of 10 or less</li> </ul>
<b>Intellectual Property Rights or IPR</b>	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> <li>• copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</li> <li>• applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>

<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
<b>Law</b>	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.

<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement Schedule 6.
<b>Material Breach</b>	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.

<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
---------------------------------	---

<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.



<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the UK GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the UK GDPR.
<b>Platform</b>	The government marketplace where Services are available for Buyers to buy.
<b>Processing</b>	Takes the meaning given in the UK GDPR.
<b>Processor</b>	Takes the meaning given in the UK GDPR.

<b>Prohibited act</b>	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
-----------------------	--

<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.

<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.

<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
<b>Replacement supplier</b>	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

<b>Services</b>	DfT require the Suppliers Services to improve and enhance the Buyers cloud provisions in the areas of security, automation and cloud savings, identifying improvements and developing new foundation solutions. Works will be commissioned via Statement of Works (Schedule 8)
<b>Service data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.

<b>Service description</b>	The description of the Supplier service offering as published on the Platform.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>SOW End Date</b>	the date up to and including this date when the supply of the Deliverables under the Statement of Work shall cease;
<b>SOW Start Date</b>	the date of the start of the Statement of Works as stated in the SOW;
<b>Statement of Work or (SOW)</b>	the document which, upon its execution by the Buyer and Supplier, shall become incorporated into their Call-Off Contract and outlines the agreed body of works to be undertaken as part of the Call-Off Contract Deliverables. There may be any number of Statements of Work incorporated into a Call-Off Contract and each Statement of Work may include (but is not limited to) the Statement of Requirements, identified output(s), completion date(s) and charging method(s);
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls">https://www.gov.uk/service-manual/agile-delivery/spend-controls</a> <del>ck-if-you-need-approval-to-spend-money-on-a-service</del>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.

<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

<b>Supplier staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
<b>Supplier Terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.

<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

## Schedule 7: Data Protection



Cabinet Office

# Procurement Policy Note – Updated Guidance on Data Protection Legislation

Action Note PPN 03/22  
2022

December

## Issue

1. The UK's exit from the European Union and changes to the data protection legal framework require updates to the data processor clauses that are a requirement under Article 28 UK GDPR. This includes recent European Court of Justice decisions regarding international transfers of personal data and the approval by Parliament of a new UK International Data Transfer Agreement (IDTA) governing the export of personal data from the UK.
2. This Procurement Policy Note (PPN) updates and replaces PPN 02/18. It contains streamlined guidance, and updated legal clauses to take into account our exit from the EU. It also includes guidance on international transfers of personal data.

## Dissemination and scope

3. The contents of this PPN apply to all Central Government Departments, their Executive Agencies and Non-Departmental Public Bodies. Together these are referred to in this PPN as 'In-Scope Organisations'. The Devolved Administrations and NHS organisations are not in scope of this PPN, however many public bodies will also be subject to data protection legislation and may wish to apply the approaches set out in this PPN.
4. In-Scope Organisations should circulate this PPN widely across their organisations, and work closely with Data Protection/Information Assurance leads within their organisations on implementation.

## Timing



5. Relevant contracts should be updated with the new clauses at Annex A when they come to be naturally renewed. If a contract involves a substantial volume of personal data, or is otherwise high risk, In-Scope Organisations may wish to introduce the new clauses via a contract variation. New contracts should use the new clauses at Annex A immediately.

## Action

6. In line with data protection law, In-Scope Organisations should already have identified existing contracts involving processing personal data and included in them the clauses provided in PPN 03/17 or PPN 02/18.

7. For contracts to be awarded after the issue of this PPN, In-scope organisations should use the updated clauses at Annex A to this PPN. Crown Commercial Service will make changes to overarching Commercial Agreements where necessary and communicate this via usual customer channels. You should also ensure any call-offs are suitably covered with appropriate clauses.

## Key considerations

### Data protection legal framework

8. The primary UK legal data protection framework is now the UK General Data Protection Regulation (UK GDPR). UK GDPR is similar to EU GDPR, but it has been amended to remove references to European organisations and laws.

9. The Data Protection Act 2018 contains clarifications and exemptions to UK GDPR, and both pieces of legislation need to be read alongside each other.

10. The Data Protection Act 2018 includes, at Part 3, the legal framework for the processing of personal data for law enforcement purposes, and at Part 4, the legal framework for the processing of personal data by the intelligence agencies.

11. There are also limited circumstances in which EU GDPR could apply to an In-Scope Organisation, where it was offering goods or services to EU citizens. In these cases, In-Scope Organisations must comply with both UK GDPR and EU GDPR. If this applies to your organisation then advice should be sought from your data protection team or Data Protection Officer.

### Controllers and Processors

12. The UK GDPR applies to 'Controllers' and 'Processors'.

- a **Controller** is a legal person or organisation which determines the purposes and means of processing personal data. A Controller is the organisation in control of the processing of personal data, who makes the key decisions, and is usually the organisation that decides to collect the personal data in the first place. It will also typically determine the specific personal data to be collected, held or used, and the

appropriate legal basis of the processing, as well as how long the data will be processed, and who the data shall be shared with.

- a **Processor** is a legal person or organisation which processes personal data on behalf of a Controller. A Processor will not be responsible for making the key decisions about the personal data and will only be processing the data under the direct, or implied, instructions of the Controller. Therefore, the Processor will not be processing any of the Controller's data for any of its own purposes, and has no direct interest in the data itself. The Processor may be providing its expertise to the Controller in respect of technical or other matters, and may have scope to make some decisions about the manner in which personal data is processed, but only to the extent that the contract with the Controller allows.

13. A Controller-Processor is likely to be the appropriate relationship in the vast majority of Buyer-Supplier relationships. In most cases in public sector contracts, the public body letting a contract or calling-off from a Framework Agreement will be the Controller, and the supplier will be the Processor.

14. Different legal obligations apply depending on the nature of the relationship with the supplier. Where the supplier is a Processor, there is a legal obligation under Article 28 UK GDPR to have a contract with the Processor and for it to contain specific data protection clauses. Part 2 of Annex A contains the clauses required by law in a Controller-Processor relationship.

### **Crown to Crown data agreements**

15. Where a Crown department acts as a Processor for another Crown department, Section 209(2) of the Data Protection Act 2018 stipulates that each Crown department is a separate Controller in law. As a matter of law, the Crown cannot contract with itself.

16. Section 209(3) of the Data Protection Act 2018 resolves this by providing that where the UK GDPR or the 2018 Act requires the relationship between Controller and Processor to be governed by a contract, a Memorandum of Understanding (MoU) will be sufficient; the MoU must include the clauses at Annex A of this PPN.

### **Joint or Independent Controllers**

17. In a limited number of circumstances, a supplier may be acting as a Joint Controller (jointly determining the purposes and means of processing) or as a Controller in their own right rather than a Processor. Where you suspect that this is the case, consult your local data protection team or Data Protection Officer for advice. In these scenarios the clauses at Annex A are unlikely to be appropriate and you should take advice from your data protection team or Data Protection Officer on the data protection provisions you should have in place.

### **Cost of compliance**

18. Any organisation required to comply with Data Protection Legislation may incur costs in doing so. Suppliers will be expected to manage their own costs in relation to compliance. In-Scope Organisations are advised not to routinely accept contract price

increases from suppliers as a result of work associated with compliance but should apply commercial judgement in individual discussions on this with suppliers.

### **Risks of non-compliance**

19. In-Scope Organisations who do not comply with data protection law will be in breach of the regulations and at risk of being fined, or having an enforcement order issued against them, by the Information Commissioner's Office (ICO).

20. Under the UK GDPR, Processors have direct legal obligations to comply with data protection law, and they can be fined by the ICO. Both Controllers and Processors can also face private claims for compensation where they have not complied with their obligations under UK GDPR.

### **Contract liabilities**

21. In-Scope Organisations should not accept liability clauses where Processors are indemnified against fines or claims under UK GDPR. The legal penalty regime has been extended directly to Processors to ensure better performance and enhanced protection for personal data, therefore entirely indemnifying Processors for any regulatory fines from the ICO or civil claims from data subjects undermines these principles.

22. As the UK GDPR gives Processors responsibilities and liabilities in their own right, Processors, as well as Controllers, may now be liable to pay damages or be subject to fines or other penalties from the ICO. In addition to the maximum regulatory fines, the increased rights of data subjects under the UK GDPR may also lead to greater exposure to civil claims for data protection breach. In-Scope Organisations should consider reviewing liability and indemnity provisions on a contract by contract basis if there is a risk that they might otherwise prevent recovery of these costs. In-Scope Organisations should consider this in accordance with the nature of the procurement, the appetite for risk and the type of personal data involved in the contract.

23. There are a range of options to be considered, to ensure the Controller is able to recover the full costs of civil data protection claims or regulatory fines issued by the ICO, where the processor is at fault, and these might include:

- excluding all data protection breaches from the general cap on liability
- increasing the general cap on liability to ensure it covers higher regulatory fines
- having a separate cap on liability for all data protection breaches
- introducing a separate £17.5 million cap on liability for regulatory fines arising out of data protection breach

24. When varying existing contracts, In-Scope Organisations should apply commercial judgement when considering whether substantial changes or additions to liability and indemnity clauses should be made in accordance with the Change in Law provisions in contracts. The existing provisions may be sufficient to cover-off the risk.

### **Expired / legacy contracts**

25. There may be some instances where personal data is still being processed by a Processor, for example it may be stored by the processor, even though the contract has expired. Data being processed in such circumstances is in breach of the legal obligation to have a contract in place where a Processor is used to process personal data. It is also in breach of the data processing principles, which Controllers are responsible for compliance with, as such storage is no longer necessary. Without a contract, it is possible that a Controller will not be meeting its obligations to ensure data security. In such circumstances you should take advice from your data protection team or Data Protection Officer. Unless the buyer and supplier are in agreement that the necessary clauses have survived the original contract covering the data processing, it is likely that an interim contract will need to be put in place; however, this should only be a temporary measure and steps must immediately be taken to ensure that any data which it is no longer necessary to process (including storage) is returned to the Controller and/or deleted. These provisions will protect the data and ensure that the Controller and Processor agree on their roles and responsibilities. This may need to exist as a separate contract if the existing contract has already expired.

### **Protective measures**

26. As set out in Article 28(3)(c) UK GDPR, Processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and these are defined as 'Protective Measures' within Annex A.

27. In-Scope organisations may consider using security schedules for contracts involving personal data processing, to provide a framework to ensure comprehensive assurance of a Processor's compliance. Controllers may reject a Processor's proposed measures if they think they are insufficient. Examples of the security considerations are at Annex B.

### **Data processing outside the UK**

28. Article 44 of UK GDPR prohibits the off-shoring of personal data outside the UK unless a legal gateway is in place. Valid legal gateways include:

- an adequacy decision<sup>1</sup> by the UK Government in respect of the destination country
- EU Standard Contractual Clauses<sup>2</sup> (until 21 March 2024 if the contract was concluded on or before 21 September 2022) or the UK International Data Transfer Agreement (IDTA)<sup>3</sup> between the data exporter and importer organisations

---

<sup>1</sup>For a list of territories granted adequacy see: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy>

<sup>2</sup> SCCs as set out in European Commission Decision 2001/497/EC and European Commission Decision 2010/87/EU.

<sup>3</sup><https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx>

- binding corporate rules where data is exported from one part of a group of companies to another member of that group and the rules have been approved by the Information Commissioner
- a legally binding and enforceable instrument between public authorities
- transfers pursuant to a Code of Conduct approved by the Information Commissioner (none currently exist)
- transfers pursuant to a certification mechanism approved by the Information Commissioner

29. If your contract does involve data being offshored outside the UK, you should identify the legal gateway that the supplier is relying on to make that lawful. The most common legal gateways that you will be relying on are an adequacy decision and Standard Contractual Clauses/IDTA.

### Adequacy decisions

30. The UK Government has declared that the European Union and European Economic Area are adequate for data protection purposes. Likewise the European Commission has also declared that the UK is adequate for data protection purposes. This means that personal data can flow unfettered between the UK and the EU/EEA.

31. The UK government has also provisionally made an [adequacy decision](#) in respect of the countries that the EU considers adequate. These include New Zealand, Israel, Switzerland, and Argentina. Limited adequacy decisions have also been made in respect of Japan and Canada.

### EU Standard Contractual Clauses (SCCs)

32. Sometimes called “Model Clauses”, these are clauses approved by the Information Commissioner and UK Government that ensure protection for data by contractual means where the destination country has not been deemed adequate. Where these clauses are in place (either as part of the contract or as a separate agreement), personal data can be exported from the UK to the supplier.

33. The EU GDPR Standard Contractual Clauses approved by the European Commission (Decisions 2001/497/EC and 2010/87/EU) have been transitionally recognised as a legally valid gateway under UK GDPR, and you can continue to rely upon these SCCs until 21 March 2024 if the contract was concluded on or before 21 September 2022. In order to rely upon the SCCs, the processing operations that are the subject matter of the contract must remain unchanged and reliance on those clauses must ensure that the transfer of personal data is subject to appropriate safeguards.

### UK International Data Transfer Agreement (IDTA)

34. On 21 March 2022 the UK government commenced a new legal instrument that provides protection for personal data exported from the UK where an adequacy decision

was not available. The International Data Transfer Agreement (IDTA) is essentially the UK version of Standard Contractual Clauses.

35. The IDTA comes in two forms:

- a. A stand-alone IDTA that covers exports of personal data from the UK.
- b. A form of IDTA that “plugs in” as an addendum<sup>4</sup> to the EU SCCs. The second version is appropriate where data may be transferred to a non-adequate territory from both the UK and EU/EEA.

36. For new contracts concluded after 22 September 2022 you must use one of the two forms of IDTA. For existing contracts or those concluded on or before 21 September 2022 you may continue to rely on the EU SCCs, but only until 21 March 2024.

### The Schrems 2 case

37. In July 2020, the European Court of Justice struck down the partial adequacy decision (“Privacy Shield”) made by the European Commission in respect of the USA. The court took the view that the USA’s surveillance legislation was disproportionate and thus personal data could not be safely exported to the USA under that decision.

38. The court also reviewed the issue of transfers of personal data to the USA which were protected by EU Standard Contractual Clauses. The court affirmed that EU SCCs were a valid transfer mechanism, but found that in relation to certain countries (like the USA) EU SCCs might need to be supplemented by additional protections in order for transfers to be lawful.

39. The UK ICO has not issued a blanket prohibition on offshoring (i.e transferring) personal data to the USA. The ICO has consulted<sup>5</sup> on draft guidance on conducting risk assessments for international transfers to assess when supplementary protections may be necessary. This guidance has not been published in its final form. The draft guidance asks that controller organisations consider a range of risk factors relating to non-adequate countries, including whether there are partial UK adequacy regulations in relation to that country, its human rights record, its legal and court system, and how close those systems are to the UK legal and court system, how overseas judgments are recognised and enforced; and its laws and practices regulating third parties access (including public authority surveillance). The ICO recognises that conducting such an assessment is not straightforward, and you should consult your data protection team for advice where data is to be transferred from or accessed from a non-adequate country.

### **The Law Enforcement Directive (LED)**

---

<sup>4</sup><https://ico.org.uk/media/for-organisations/documents/4019535/addendum-international-data-transfer.docx>

<sup>5</sup><https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf>

40. Part 3 of the Data Protection Act 2018 applies in relation to domestic and cross-border processing of personal data for law enforcement purposes. Similar obligations apply as under UK GDPR, but there are some significant differences, in particular in relation to the storage and classification of data. The ICO has produced [guidance](#) on law enforcement processing.

41. Whilst the standard generic clauses at Annex A are compliant with the requirements of Part 3 of the Data Protection Act 2018, In-Scope Organisations engaged in processing personal data for law enforcement purposes as Controllers may require more specific drafting in contracts to flow some of these obligations down to their Processors. Legal advice should be sought in these cases.

## **Sources of Further Information**

42. The Information Commissioner's Office is a useful source of latest information on data protection law. Other sources of information are listed below:

[ICO Information on UK GDPR](#)

[General Data Protection Regulations](#)

[ICO guidance on law enforcement processing](#)

[UK GDPR](#)

## **Contact**

43. Commercial and procurement enquiries associated with this PPN should be directed to the Crown Commercial Service Helpdesk on 0345 410 2222 or [info@crownccommercial.gov.uk](mailto:info@crownccommercial.gov.uk).

44. Enquiries on UK GDPR should be directed to your data protection team, Data Protection Officer, or the Information Commissioner's Office (on 0303 123 1113 or via their [Live Chat](#) service, available through their website).

## **Annex A - Part 1: Generic Standard UK GDPR Clauses**

**Customer:** Department for Transport

**Contractor:** Opus 2 International Ltd

**Party:** Party to this Agreement

**Agreement:** this contract;

**Law:** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

**Processor Personnel:** means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement.

### **GDPR CLAUSE DEFINITIONS:**

**Data Protection Legislation:** (i) all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (ii) (to the extent that it may be applicable) the EU GDPR). The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018.

**Data Protection Impact Assessment:** an assessment by the Controller carried out in accordance with Section 3 of the UK GDPR and sections 64 and 65 of the DPA 2018.

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer** take the meaning given in the UK GDPR.

**Data Loss Event:** any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

**Data Subject Request:** a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access their Personal Data.

**DPA 2018:** Data Protection Act 2018

**UK GDPR:** the UK General Data Protection Regulation

**Joint Controllers:** takes the meaning given in Article 26 of the UK GDPR

**Law Enforcement Processing:** processing under Part 3 of the DPA 2018.

**Protective Measures:** appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Agreement, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems



and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (Security).

**Sub-processor:** any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement.

## **1. DATA PROTECTION**

1.1 The Parties acknowledge that for the purposes of Data Protection Legislation, the Customer is the Controller, and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Schedule 20 by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR.

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

1.3 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:

- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
- (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

- (a) process that Personal Data only in accordance with Schedule 20, 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;
- (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;

- (iii) state of technological development; and
- (iv) cost of implementing any measures;
- (c) ensure that :
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 20;
  - (ii) 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:
    - (A) are aware of and comply with the Processor's duties under this clause;
    - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
    - (C) 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 this Agreement; and
    - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
  - (d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
    - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
    - (ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
    - (iii) the Data Subject has enforceable rights and effective legal remedies;
    - (iv) the Processor complies with its obligations under Data Protection Legislation by providing an appropriate 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
    - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
  - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Request (or purported Data Subject Request);
- (b) receives a request to rectify, block or erase any Personal Data;

- (c) receives any other request, complaint or communication relating to either Party's obligations under Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- (e) 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
- (f) becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in Data Protection Legislation;
- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Data Loss Event;
- (e) 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.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

- (a) the Controller determines that the processing is not occasional;
- (b) 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
- (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10 Each Party shall designate its own data protection officer if required by Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

- (a) notify the Controller in writing of the intended Sub-processor and processing;
- (b) obtain the written consent of the Controller;
- (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Sub-processor; and
- (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may upon giving the Processor not less than 30 working days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

## Annex A - Part 2: Schedule of Processing, Personal Data and Data Subjects (Schedule 11)

### **Schedule 11 Processing, Personal Data and Data Subjects**

This Schedule 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 Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are:  
[REDACTED]
2. The contact details of the Processor's Data Protection Officer(s) are: [REDACTED]  
[REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	<i>The Parties acknowledge that for the purposes of Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1.</i>
Subject matter of the processing	<i>The processing is needed to ensure that the Processor can effectively deliver the contract to provide document management, transcription and overseas support services to the Cranston Inquiry.</i>
Duration of the processing	<i>Duration of the Call-Off Agreement unless the expiry date of this Call-Off is revised with the agreement of the contracting parties</i>
Nature and purposes of the processing	<i>The purpose of processing this data is to comply with a legal obligation.</i>  <i>The provision of the Services, as described in the Specification, including (without limitation):</i> <ul style="list-style-type: none"><li>● <i>Provision of document management platform and associated project and technical support</i></li></ul>

	<ul style="list-style-type: none"> <li>• <i>Provision of Hearing Room services including real-time transcription and Electronic Presentation of Evidence</i></li> <li>• <i>Provision of venue and live audio-visual connection between the UK and overseas location(s).</i></li> </ul>
Type of Personal Data being Processed	<p><i>The personal data transferred may concern the following categories of data:</i></p> <ul style="list-style-type: none"> <li>• <i>Surname, first name, suffix</i></li> <li>• <i>Contact data (e.g. telephone number, e-mail address)</i></li> <li>• <i>Address</i></li> <li>• <i>Date of birth</i></li> <li>• <i>Education and professional qualification</i></li> <li>• <i>Information on occupation and employment</i></li> <li>• <i>Professional connections</i></li> <li>• <i>Nationality</i></li> <li>• <i>Personal preferences and interests</i></li> <li>• <i>Physical location of the person</i></li> <li>• <i>Dates, calendar entries</i></li> <li>• <i>Online ID, tracking cookies, IP addresses</i></li> <li>• <i>Racial or ethnic origin, including dress</i></li> <li>• <i>Religious and philosophical and ideological belief</i></li> <li>• <i>Cultural identifiers</i></li> <li>• <i>Political opinions, allegiance or belief</i></li> <li>• <i>Union membership</i></li> <li>• <i>Health and medical records, including biometrics and genetics</i></li> <li>• <i>Sexual orientation and sex life</i></li> <li>• <i>Photographs</i></li> <li>• <i>Police clearance certificates or other data on criminal offences</i></li> </ul>
Categories of Data Subject	<p><i>As above. Also, staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.</i></p>

International transfers and legal gateway	<i>All data to be processed within the EEA.</i>
Plan for return and destruction of the data once the processing is complete	<i>Data will be retained for the duration of the contract.</i>  <i>The contracting parties are to agree the decommissioning process, including timelines for the secure destruction of data.</i>

## **Annex B: Security**

The technical security requirements set out below provide an indication of the types of security measures that might be considered, in order to protect Personal Data. More, or less, measures may be appropriate depending on the subject matter of the contract, but the overall approach must be proportionate. The technical requirements must also be compliant with legislative and regulatory obligations for content and data, such as UK GDPR.

The example technical security requirements set out here are intended to supplement, not replace, security schedules that will detail the total contractual security obligations and requirements that the Processor (i.e. a supplier) will be held to account to deliver under contract. Processors are also required to ensure sufficient 'flow-down' of legislative and regulatory obligations to any third party Sub-processors.

**External Certifications e.g.** Buyers should ensure that Suppliers hold at least Cyber Essentials Plus certification and ISO 27001:2013 certification if proportionate to the service being procured.

**Risk Assessment e.g.** Supplier should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

**Security Classification of Information e.g.** If the provision of the Services requires the Supplier to Process Authority/Buyer Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Supplier shall implement such additional measures as agreed with the Authority/Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

### **End User Devices e.g.**

- The Supplier shall ensure that any Authority/Buyer Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority/Buyer except where the Authority/Buyer has given its prior written consent to an alternative arrangement.
- The Supplier shall ensure that any device which is used to Process Authority/Buyer Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

**Testing e.g.** The Supplier shall at their own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Authority/Buyer data being transferred into their systems. The ITHC scope must be agreed with the Authority/Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority/Buyer data.

**Networking e.g.** The Supplier shall ensure that any Authority/Buyer Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.



**Personnel Security e.g.** All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier maybe required to implement additional security vetting for some roles.

**Identity, Authentication and Access Control e.g.** The supplier must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The supplier must retain records of access to the physical sites and to the service.

**Data Destruction/Deletion e.g.** The Supplier must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority/Buyer data has been stored and processed on.

**Audit and Protective Monitoring e.g.** The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority/Buyer Data. The retention periods for audit records and event logs must be agreed with the Authority/Buyer and documented.

**Location of Authority/Buyer Data e.g.** The Supplier shall not, and shall procure that none of its Sub-contractors, process Authority/Buyer Data outside the EEA without the prior written consent of the Authority/Buyer and the Supplier shall not change where it or any of its Sub-contractors process Authority/Buyer Data without the Authority/Buyer's prior written consent which may be subject to conditions.

**Vulnerabilities and Corrective Action e.g.** Suppliers shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

Suppliers must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

**Secure Architecture e.g.** Suppliers should design the service in accordance with:

- NCSC "[Security Design Principles for Digital Services](#)"
- NCSC "[Bulk Data Principles](#)"
- NSCS "[Cloud Security Principles](#)"

## Schedule 8 – Statement of Works Template

### Annex 1 (Template Statement of Work)

#### 1 Statement of Works (SOW) Details

Upon execution, this SOW forms part of the Call-Off Contract (reference below).

The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.

All SOWs must fall within the Specification and provisions of the Call-Off Contract.

The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.

<b>Date of SOW:</b>	<b>17/4/2024</b>
<b>SOW Title:</b>	<b>Cranston Inquiry – Hearings.</b>
<b>SOW Reference:</b>	<b>TMAR3112</b>
<b>Call-Off Contract Reference:</b>	<b>TMAR3112</b>
<b>Buyer:</b>	<b>[REDACTED] (Budget Holder)</b> <b>[REDACTED] (main point of contact)</b>
<b>Supplier:</b>	<b>Opus 2 International Limited</b>
<b>SOW Start Date:</b>	<b>09<sup>th</sup> May 2024</b>
<b>SOW End Date:</b>	<b>08<sup>th</sup> May 2025</b>
<b>Duration of SOW:</b>	<b>1 week TBC (family meetings abroad)</b> <b>4-6 weeks TBC (hearings in London)</b>
<b>Key Personnel (Buyer):</b>	<b>[REDACTED]</b>
<b>Key Personnel (Supplier):</b>	<b>[REDACTED] - Head of Technical Services</b> <b>[REDACTED] – Case Manager &amp; Public Inquiry Consultant</b>

	<b>██████████ – Senior Business Development Associate</b>
<b>Subcontractors:</b>	<b>N/A</b>

## 2 Call-Off Contract Specification – Deliverables Context

### 2.1 SOW Deliverables Background:

The Supplier will provide:

- (i) specialist electronic Hearings ('trial') management to support the Buyer's Inquiry operations until the anticipated completion of Hearings; and
- (ii) Full support to enable video conferencing of pre-meetings with family members overseas and video streaming of Hearings taking place in London. Overseas locations likely to include the Kurdish region of Iraq and possibly other locations.

Service provision should be in accordance with the Opus 2 'Complete' solution tier, as described in the Opus 2 GCloud Service Definition Document, and include:

#### **A) Provision of document management platform**

- 1. Preparation of Public Inquiry Workspace
- 2. Content Management and Technical Support
- 3. Project Management
- 4. Platform access
- 5. Data Hosting
- 6. Training
- 7. Additional Workspaces

#### **B) Hearing Room Services**

- 1. Transcription (court reporting)
- 2. Real time connections to live transcript
- 3. Electronic Presentation of Evidence (EPE)
- 4. Audio or audio-visual recording, where required.
- 5. Case management and technical support

#### **C) Overseas support**

- 1. Sourcing of appropriate venue to hold remote meetings/Hearings.

Full support to enable video conferencing of pre-meetings with family members overseas and video streaming of Hearings taking place in London. Overseas locations likely to include the Kurdish region of Iraq and possibly other locations.

## **2.2 Delivery phase(s):**

### **Document Management**

The Supplier will provide document management services, uploading documents to form the eventual Inquiry Bundle and supporting users with their use of the platform. Once the document set is largely ready, the documents and metadata should be exported from the eDisclosure platform (Relativity operated by Epiq) and sent to the Supplier where the Supplier will upload them to their document management platform, allowing for the construction and hosting of the Bundle. Note - this general workflow may need to be repeated for any future additions / changes once the initial Bundle has been created.

The Supplier and the Inquiry legal team will work together to structure the Bundle, the Supplier will offer best practice advice for the use of an electronic bundle during the Inquiry and on any particular functionality, e.g. utilising hyperlinking, custom bundles and tagging etc, that may aid the Inquiry's work. This will enable users to navigate through the Bundle folders to begin annotating and tagging the documents with the rest of their team, in preparation for the hearing.

### **Realtime Transcription and Evidence Presentation**

The Supplier will take an audio feed from the AV provider, RTS, this audio will be recorded and used to produce a transcript and allow for editing of the draft transcript to produce a final transcript (the draft transcript will be seen live as Realtime transcription that individual users can annotate).

The Supplier will install EPE (Electronic Presentation of Evidence) services and will be responsible for the display of evidence during the hearings. Opus 2 will provide equipment for users on request.

### **Overseas Support**

The supplier will provide a live audio-visual connection between venue(s) that the supplier will procure abroad (likely to be the Kurdish region of Iraq and possibly elsewhere) and the London Hearing venue, enabling full connectivity for a Hearing held across two venues.

### 2.3 Overview of Requirement:

To provide document management, transcription and overseas support services to the Cranston Inquiry at meetings and public Hearings.

## 3 Buyer Requirements – SOW Deliverables

### 3.1 Outcome Description:

Deliverables	Outcome	Acceptance Criteria
D1	<b>Document Management</b> Securely handle and store Inquiry documents. Access restrictions and confidential documents to be flagged, as advised by the Inquiry.	Clear understanding of data protection requirements identified by Supplier in working protocols and practices.
D2	<b>Evidence Presentation</b> Bundles to be created in accordance with instructions from Inquiry lawyers. Documents to be presented cleanly and with minimal delay to ensure smooth running of Inquiry hearings. Inquiry users to be able to notate and annotate documents in their own workspace.	Evidence that the Supplier understands and has good experience of providing Electronic Presentation of Evidence for public inquiries or similar hearings.

<b>D3</b>	<b>Setup</b> Hearing venue to be set up no later than one working day in advance of hearing. Opus to provide hardware.	Evidence that the Supplier can provide relevant hardware that is set up, tested and fully functioning to the Inquiry's satisfaction by the time required.
<b>D4</b>	<b>Transcription</b> Realtime transcriptions of Inquiry hearings combined with integrated Bundle and evidence presentation.	Evidence that the Supplier can provide high quality realtime transcription services alongside integrated Bundle and evidence presentation, all capable of being annotated by individual users.
<b>D5</b>	<b>Overseas Support</b> Procure appropriate venue(s) to hold remote meetings. Provide audio-visual and Hearing Room services for high quality live connection between UK and overseas location(s).	Evidence of similar previous activity, including in environments where personal safety and security are an important issue.
<b>D6</b>	<b>Additional services outlined in the Supplier Service Offering may be called off during the contract life.</b>	

### 3.3.1 Milestones:

The milestones for the deliverables identified within this SOW are listed in 3.3.2.

### 3.3.2 Delivery Sign-off:

See Call-Off contract Start and end date.
<b>D1-D6</b>
Accepted / Rejected – Progress signed off by the Business Manager on monthly reviews.
Signed/Date by DfT Delivery Manager

### 3.4 Dependencies:

<b>DP1</b>	Dates – Secretariat to identify dates for London and overseas Hearings and any other overseas meetings.
<b>DP2</b>	Hearing venue (London) – Secretariat to source and procure suitable Hearing venue.
<b>DP3</b>	Hearing / Meeting venue(s) (overseas) – Opus to source and procure suitable venue(s).
<b>DP4</b>	Relativity access – Opus will upload documents from Relativity (operated by Epiq). Both parties need to ensure connectivity and relevant timescales for Hearings.

### 3.5 Supplier Resource Plan:

Role Description	Day Rate (excluding VAT)	No of Days	Total Charge
Technical Consultancy	████ per hour	TBC	TBC

Reporting Team Attendance	■	TBC	TBC
EPE Operator	■	TBC	TBC
Virtual Hearing Manager (for preliminary meetings)	■	TBC	TBC
		<b>Total</b>	<b>TBC</b>

### 3.6 Security Applicable to SOW:

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables have completed Supplier Staff Vetting in accordance with the Call-Off Agreement.

All Supplier Staff to sign written undertaking about safety and security of Inquiry documents. Inquiry Secretariat will provide the template.

#### 3.6.1 Cyber Essentials Scheme:

The Buyer requires the Supplier to have and maintain a Cyber Essentials Certificate for the work

undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

The Supplier Staff must adhere to the Cyber Security standards, protocols & ISO/IEC27001 – Information Security Management:

<https://www.gov.uk/government/publications/the-minimum-cyber-security-standard> <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles> <https://www.ncsc.gov.uk/cyberessentials/overview>

### 3.7 Additional Requirements:

The buyer can request additional services anytime during the term of the contract.



### 3.8 Key Supplier Staff:

Key Role	Key Staff
Technical Support	<div>██</div> <div>██</div> <div>██</div> <div>██</div> <div>(Wider Technical Team as applicable)</div>
Transcription Services	Reporting Team comprising of one stenographer and one editor – names to be provided once sitting dates confirmed.
Evidence Presentation (EPE)	EPE Operator – name to be provided once sitting dates confirmed.
Virtual Support (for preliminary meetings)	<div>██████████ – Audio Visual (AV) Services &amp; Quality Assurance Manager</div> <div>██████████ – Virtual Hearing Manager</div>

## 4 Charges

### 4.1 Call Off Contract Charges:

The applicable charging method(s) for this SOW is:

Capped Time and Materials	See Schedule 2: Call-Off Contract charges
---------------------------	---

**Rate Cards Applicable:** The rate cards agreed within the main body of the Call Off Contract will apply. (See Schedule 2: Call-Off Contract charges)

### 4.2 Reimbursable Expenses:

Any claim(s) for Travel and Subsistence will be agreed upfront by both the Supplier and DfT in writing before proceeding in all circumstances. All claims that have not been agreed will be rejected. Claims for Travel and Subsistence are based on DfT's standard rates referred in Call-off schedule 5 only. All invoices received will require management information to support the claim.

Payment milestones will be aligned to deliverable milestones as per 3.3.2:

SOW 01 –	<p>All fees related to this SOW are contained in Schedule 2: Call-Off Contract charges.</p> <p>Fees will be invoiced monthly in arrears in accordance with service deliverables defined in the deliverable milestones in 3.3.2</p> <p>Both parties agree that if any of the DfT Buyer Responsibilities listed under the Order Form and in this SOW or DfT risks laid out in this document prevent or delay Supplier deliverables, then the Supplier will not be held responsible. The Supplier will be entitled to continue to bill as per the section 4.2 of this SoW, subject to prior agreement with DfT.</p>
----------	--

The Supplier will invoice the Buyer monthly, on a Time and Materials basis for the previous months efforts against the Deliverables set out in 3.3.1 – Schedule / Milestones of Deliverables. It will be the responsibility of the DFT Senior Delivery Manager to sign-off all agreed milestones in order to release monthly payment.

Risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges. Any new identified risks by the supplier or buyer during delivery will be discussed and if agreed will be added

**4.3 Risks:**

Ref;	Description	Likelihood	Severity	Date
R1	The Inquiry has to be adjourned for a lengthy period requiring the contract to be re-negotiated.	Low	Medium	11/04/24
R2	Uncertainty over Hearing dates and venues makes forward planning uncertain.	Medium	Low	11/04/24
R3	Technical or financial failure (including successful cyber-attack) of Epiq Systems Ltd or Opus 2 International Ltd leads to loss of service to Inquiry.	Low	High	11/04/24
R4	Technical failure (including successful cyber-attack) of DfT leads to loss of service to Inquiry.	Low	Medium	11/04/24

#### 4.4 Assumptions:

Ref ;	Description
A1	<p>Before any services are carried out, there must be an agreement between the Buyer and Supplier in terms of what is expected of the Supplier in terms of performance and deliverables, which shall be set out using the Statement of Works template in Schedule 8.</p> <p>To identify performance and deliverables, the Buyer should review the Supplier's service levels and response times provided under Schedule 1 and consider setting milestones with associated Deliverables and agreeing payments against those Deliverables, as per the Statement of Works template in Schedule 8.</p> <p>The Buyer shall also consider including Implementation, Exit and Offboarding Plans and milestones. An Exit Plan shall be provided by the Supplier within 6 months of contract start and be updated and reviewed with the Buyer at a minimum every 6 months throughout the contract term.</p>
A2	
A3	

The Supplier Staff must adhere to the Government Supplier Code of Conduct

<https://www.gov.uk/government/publications/supplier-code-of-conduct>

The Supplier Staff must adhere to Data Sharing Standards.

The Supplier Staff will work within an assigned Product Organisation and work with the Technical Product Manager, Product Lead Engineer, Product Architect.

The Supplier will provide the specific roles specified within this SOW.

#### **4.5 Governance**

Any changes to Scope, Timescales and Costs within this SOW will be managed through Variation and version control. All variations will be signed by the Supplier Representative and Senior Commercial Advisor.

#### **4.6 Intellectual Property Rights (IPR)**

Unless otherwise specified in the Call-Off Contract: Software will be developed under crown copyright, using MIT Licence. For further information on IPR, please see call off agreement.

#### **4.7 Other Requirements**

All Supplier Staff must be BPSS cleared. SC clearance may be required for further work but will be sponsored by DfT if needed. Temporary DfT email and system access will be provided and all documentation will be retained on DfT systems. A standard DfT declaration will have to be signed.

#### **4.8 Place of Performance**

The work will take place in:



- I. Overseas Support – in a location to be determined but likely to be in the Kurdish region of Iraq.
- II. Inquiry Hearings – in a London venue, to be determined.

#### **4.9. Signatures and Approvals**

##### **Agreement of this SOW**

BY SIGNING this Statement of Work, the Parties agree that it will be incorporated into Annex 1 of the Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:


For and on behalf of the Supplier:

Name:	
Title:	Chief Commercial Officer
Date:	07/05/2024
Signature:	

DfT Business Representative:

Name:	
Title:	Deputy Secretary
Date:	24/04/2024
Signature:	

For and on behalf of the Buyer, (DfT Commercial Representative):

Name:	
Title:	Procurement Business Partner
Date:	07/05/2024

Signature:	
------------	---

## **Annex 1**

### **Data Processing**

Prior to the execution of this Statement of Works, the Parties shall review Annex 2 of Joint Schedule 11 (Processing Data) contained in the main body of the contract.