



# G-Cloud 13 Call-Off Contract

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

Part A: Order Form	2
Part B: Terms and conditions	12
Schedule 1: Services	35
Schedule 2: Call-Off Contract charges	36
Schedule 6: Glossary and interpretations	37
Schedule 7: GDPR Information	49
Annex 2: Joint Controller Agreement	53
Annex 3: Everbridge Service Definition	61

## 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>	8798 9726 2853 415
<b>Call-Off Contract reference</b>	C287033
<b>Call-Off Contract title</b>	Provision of Critical Event Management Software
<b>Call-Off Contract description</b>	Mass Notification Service for the purpose of multi-modal contact and alerts
<b>Start date</b>	01/07/2024
<b>Expiry date</b>	30/06/2025
<b>Call-Off Contract value</b>	£82,500.00 excluding VAT
<b>Charging method</b>	BACS payment, annually in advance, within net 30 days.
<b>Purchase order number</b>	NHSE to provide once contract signed

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>	NHS England [REDACTED] [REDACTED] [REDACTED] [REDACTED]
<b>To the Supplier</b>	[REDACTED] [REDACTED]  Everbridge Europe Limited [REDACTED] [REDACTED] [REDACTED] [REDACTED]  [REDACTED]
<b>Together the ‘Parties’</b>	

Principal contact details

For the Buyer:

Title: [REDACTED]  
Name: [REDACTED]  
[REDACTED]

For the Supplier:

Title: [REDACTED]  
Name: [REDACTED]  
[REDACTED]  
[REDACTED]

## Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on 1 <sup>st</sup> July 2024 and is valid for 12 months expiring 30 June 2025.
<b>Ending (termination)</b>	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least <b>90</b> 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 <b>30</b> days from the date of written notice for Ending without cause (as per clause 18.1).</p> <p>In the event the Buyer terminates this Call-Off Contract prior to its expiry, the Buyer remains liable to pay all Charges hereunder.</p>
<b>Extension period</b>	<p>This Call-Off Contract can be extended by the Buyer for one period of up to <b>12 months</b>, by giving the Supplier <b>1 month</b> written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>The Charges for any extended Term will be as per the G-Cloud pricing available at the time for such extension.</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 below:</p> <p>Mass Notification Service for the purpose of multi-modal contact and alerts</p>

<b>Additional Services</b>	NA
<b>Location</b>	The Services will be delivered to Buyer sites and personnel contacts as provided to the supplier
<b>Quality standards</b>	The quality standards required for this Call-Off Contract are as per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415
<b>Technical standards:</b>	The technical standards used as a requirement for this Call Off Contract are as per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415
<b>Service level agreement:</b>	The service level and availability criteria required for this Call Off Contract are as per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415
<b>Onboarding</b>	The onboarding plan for this Call-Off Contract is as per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415
<b>Offboarding</b>	<p>The offboarding plan for this Call-Off Contract is as per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415</p> <p>The offboarding plan for this Call-Off Contract is:</p> <p>The Supplier is required to ensure the orderly transition of the service from the Supplier to the Buyer and/or Replacement Supplier in the event of termination or expiry of this contract. This section sets out the principles of the exit and service transfer arrangements that are intended to achieve an orderly transition which shall form the basis of the Exit Plan.</p> <p>The Supplier will, within 6 weeks after the award of the contract, deliver to the Buyer an Exit Plan which sets out the Supplier's proposed methodology for achieving an orderly transition of Services from the Supplier to the Buyer and/or its replacement Supplier on the expiry or termination of this contract.</p> <p>The Exit Plan will comply with the requirements set out below: Within 30 days after the submission of the Exit Plan, the parties will use their respective reasonable endeavours to agree the contents of the Exit Plan.</p>

	<p>The Exit Plan should contain as a minimum:</p> <ul style="list-style-type: none"> <li>• The management structure to be employed during both the transfer and cessation of the services</li> <li>• A detailed description of both the transfer and cessation processes, including a timetable for the transition of the Services to the Buyer and/or a Replacement Supplier.</li> </ul> <p>Before expiry of the Call-Off Contract the offboarding plan will be reviewed and defined as required by the Buyer.</p>
<b>Collaboration agreement</b>	N/A
<b>Limit on Parties' liability</b>	<p>The limitation of liability for this Call-Off Contract is stated in Clause 24 of the Terms and Conditions (Part B)</p> <p>The estimated Year 1 Charges used to calculate liability in the first Contract Year is [REDACTED]</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 [REDACTED] for each individual claim or any higher limit the Buyer requires (and as required by Law)</li> <li>• employers' liability insurance with a minimum limit of [REDACTED] or any higher minimum limit required by Law</li> <li>• public liability insurance with a minimum limit of indemnity of [REDACTED] for each individual claim</li> </ul>
<b>Buyer's responsibilities</b>	As per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415

<b>Buyer's equipment</b>	N/A
--------------------------	-----

### Supplier's information

<b>Subcontractors or partners</b>	<b>Not applicable</b>
-----------------------------------	-----------------------

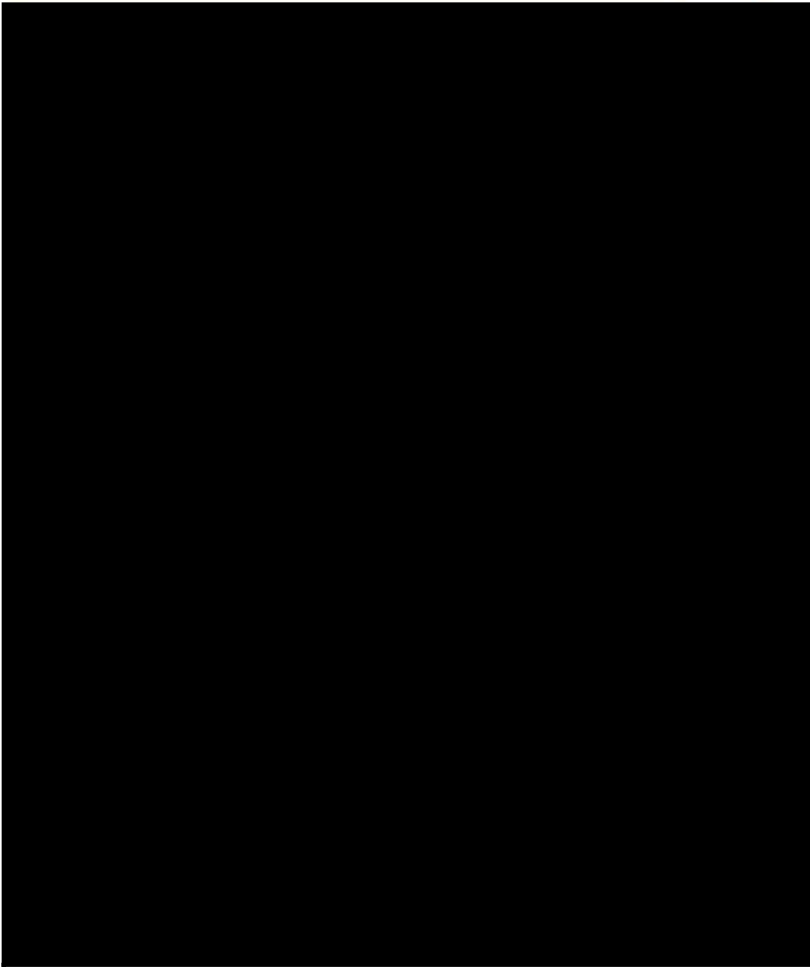
### Call-Off Contract charges and payment

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 annual invoicing in advance.
<b>Invoice details</b>	The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice
<b>Who and where to send invoices to</b>	<p>Invoices containing the NHSE Purchase Order Number or Reference Number, and addressed to:</p> <p>NHS England, [REDACTED] [REDACTED] should be submitted via Tradeshift: [REDACTED]</p> <p>If any of the supplier contact information changes during the contact period e.g. the supplier address, the supplier must notify the Buyer of these changes before submitting any future</p>

	invoices so that the purchase order can be amended as appropriate. If the information on an invoice does not match the information on the purchase order, then the invoice cannot be paid.
<b>Invoice information required</b>	<p>All invoices must include</p> <ul style="list-style-type: none"> <li>• Purchase Order Reference number</li> <li>• Contract Reference (C287033)</li> <li>• Date</li> <li>• Addresses (Buyer &amp; Supplier)</li> <li>• Supplier name and contact details</li> <li>• Remittance &amp; payment bank account details</li> <li>• Description of the charges</li> <li>• Volume of the charges</li> <li>• Unit cost of the charges</li> </ul>
<b>Invoice frequency</b>	Invoice will be sent to the Buyer annually in advance.
<b>Call-Off Contract value</b>	The total value of this Call-Off Contract is £82,500.00 (excluding VAT)



<b>Call-Off Contract charges</b>	
----------------------------------	---

Additional Buyer terms

<b>Performance of the Service</b>	As per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415
<b>Guarantee</b>	N/A
<b>Warranties, representations</b>	As per Service Definition of G-Cloud 13 Service ID 8798 9726 2853 415

<b>Supplemental requirements in addition to the Call-Off terms</b>	N/A
<b>Alternative clauses</b>	N/A
<b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b>	N/A
<b>Personal Data and Data Subjects</b>	Annex 1 of Schedule 7 is being used
<b>Intellectual Property</b>	Ref to Section 11 of Call-Off contract.
<b>Social Value</b>	Ref to Section 2.1 of Call-Off Contract

## 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 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>		
	<b>Name</b>	
	<b>Title</b>	
	<b>Date</b>	

## Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:  
[G-Cloud 13 Customer Benefits Record](#)

## Part B: Terms and conditions

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

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 periods 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 extend the contract beyond 12 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)
- 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 glossary and interpretation 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 14-digit 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.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

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 invoiced 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 [REDACTED]

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 [REDACTED] 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 [REDACTED] 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-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on  
Risk Management:  
<https://www.cpni.gov.uk/content/adopt-risk-management-approach> 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/technology-code-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 (and the Buyer of any Buyer Confidential Information breach). 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: 4.2 to 4.7 (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 the number of 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 [REDACTED] ([REDACTED]) or [REDACTED] [REDACTED] per cent ([REDACTED]%) 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.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate [REDACTED] [REDACTED] pounds [REDACTED]).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 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



29.3 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.

29.4 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.

29.5 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.

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

29.6.1 its failure to comply with the provisions of this clause

29.6.2 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

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

29.8 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.

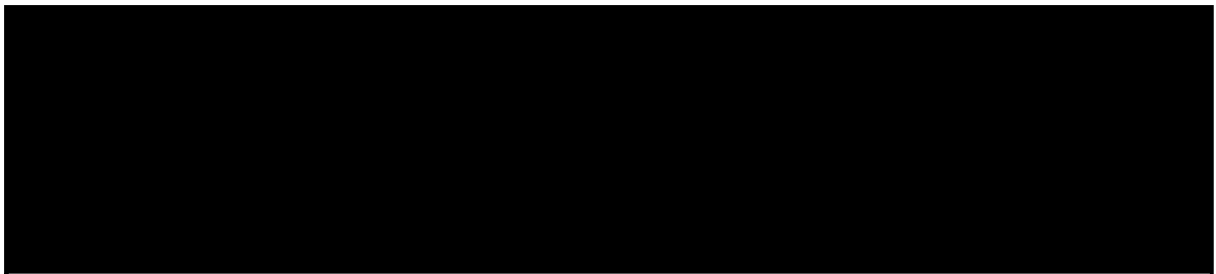
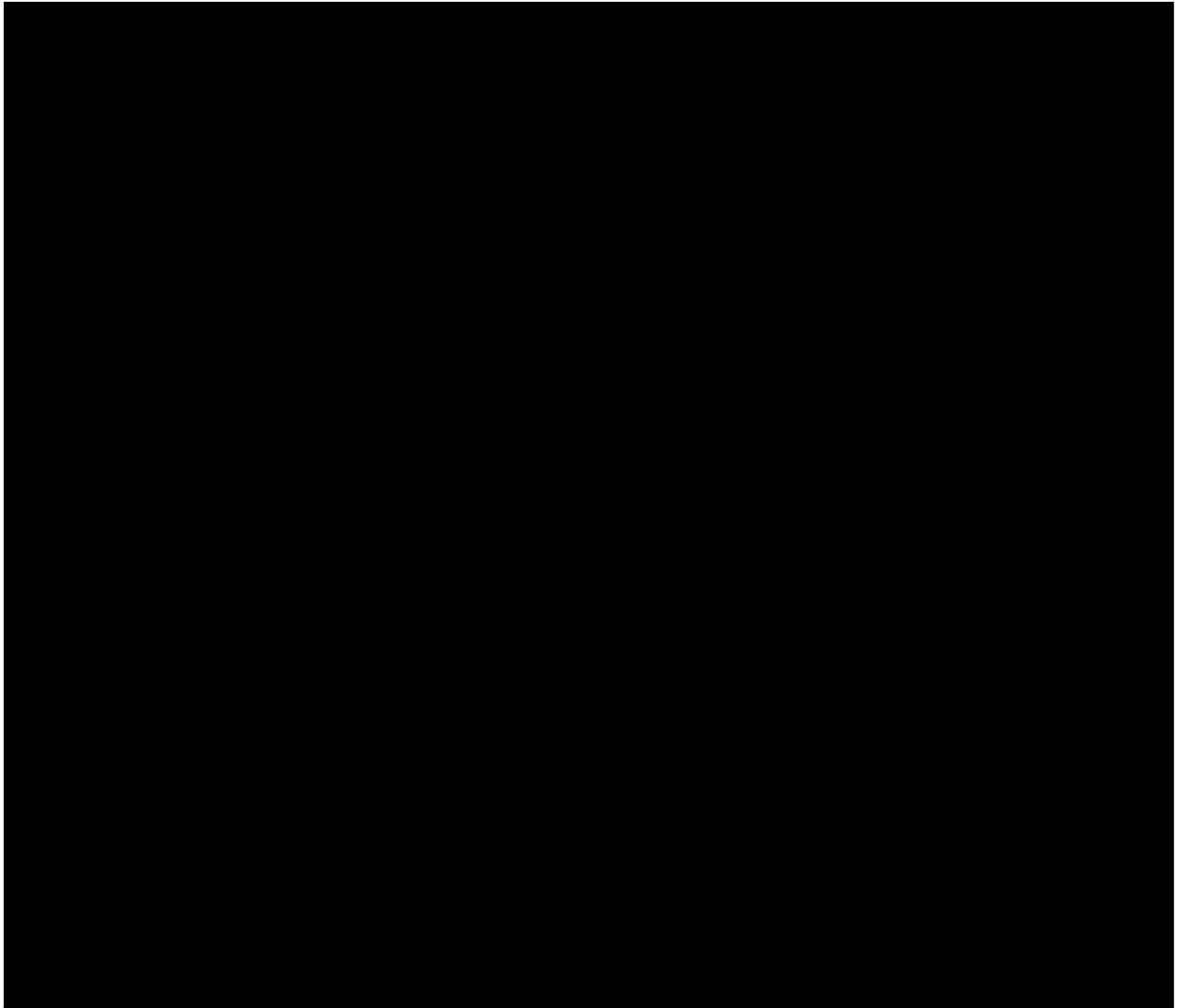
32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

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



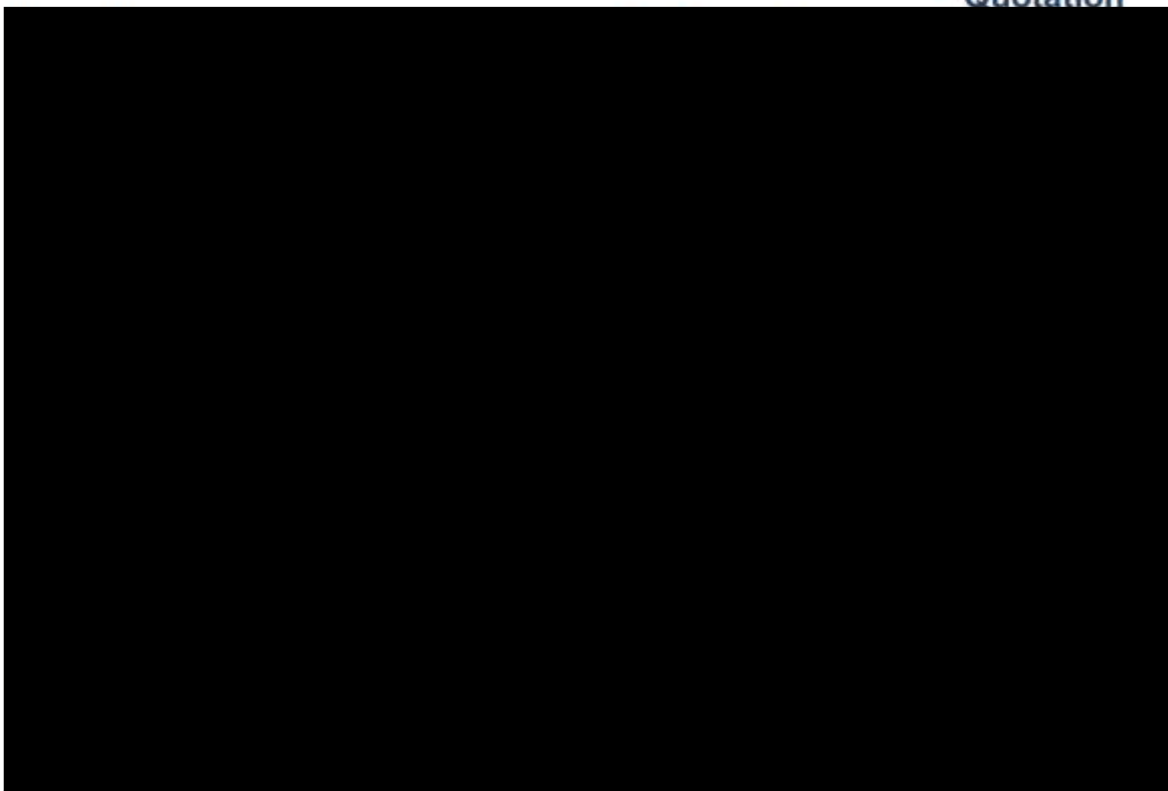
## Schedule 2: Call-Off Contract charges

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 detailed Charges breakdown for the provision of Services during the Term will include:

<https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-13/documents/93511/879897262853415-pricing-document-2022-05-06-1454.pdf>



Quotation



## 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 Offered) 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>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>	Data, Personal Data and any information, which may include (but isn't limited to) any: <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>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-for-tax">https://www.gov.uk/guidance/check-employment-status-for-tax</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 Majeure at the time this Call-Off Contract was entered into</li> <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 RM1557.12 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>	Can be: <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> </ul>
<b>Intellectual Property Rights or IPR</b>	Intellectual Property Rights are: <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>	The services ordered by the Buyer as set out in the Order Form.
<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>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-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>
<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: GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

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

- 1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
-------------	---------

Identity of Controller for each Category of Personal Data	<p><b>The Buyer is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>Names, telephone numbers, email addresses, job role, title, physical addresses, and other locations of users only as provided by Buyer for use explicitly in this Call-Off Contract.</p>
Duration of the Processing	<p><b>Up to 7 years after the expiry or termination of the Framework Agreement</b></p>
Nature and purposes of the Processing	<p>To facilitate the fulfilment of the Supplier's obligations arising under this Framework Agreement including</p> <ul style="list-style-type: none"> <li>i. Ensuring effective communication between the Supplier and CSS</li> <li>ii. Maintaining full and accurate records of every Call-Off Contract arising under the Framework Agreement in accordance with Clause 7.6</li> </ul>

Type of Personal Data	<p>Includes:</p> <ul style="list-style-type: none"> <li>i. Contact details of, and communications with, CSS staff concerned with management of the Framework Agreement</li> </ul>
	<ul style="list-style-type: none"> <li>ii. Contact details of, and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement,</li> <li>iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Agreement Contact details, and communications with Supplier staff concerned with management of the Framework Agreement</li> </ul>
Categories of Data Subject	<p>Includes:</p> <ul style="list-style-type: none"> <li>i. CSS staff concerned with management of the Framework Agreement</li> <li>ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Agreement</li> <li>iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Agreement</li> <li>iv. Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Agreement</li> </ul>

<p>Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>All relevant data to be deleted 7 years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder</p>
---	--

## Annex 2: Joint Controller Agreement

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

- 1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.
- 1.2 The Parties agree that the [**select: Supplier or Buyer**]:
- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
  - (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
  - (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
  - (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
  - (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**select: Supplier's or Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).
- 1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

## 2. Undertakings of both Parties

### 2.1 The Supplier and the Buyer each undertake that they shall:

- (a) report to the other Party every **[insert number]** months on:
  - (i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
  - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
  - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
  - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
  - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;
- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
  - (i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information
  - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
  - (iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken 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;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
  - (i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

### 3. Data Protection Breach

- 3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
  - (b) all reasonable assistance, including:
    - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
    - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
    - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
    - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.
- 3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:
- (a) the nature of the Personal Data Breach;



- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

## 4. Audit

### 4.1 The Supplier shall permit:

- (a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

### 4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

## 5. Impact Assessments

### 5.1 The Parties shall:

- (a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

## 6. ICO Guidance

- 6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30)

Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

## 7. Liabilities for Data Protection Breach

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Buyer is responsible for the

Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

- (c) if no view as to responsibility is expressed by the Information

Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the

Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

## 8. Termination

- 8.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Controller Agreement), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

## 9. Sub-Processing

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

## 10. Data Retention

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

## Annex 3: Everbridge Service Definition 8798 9726 2853 415



### **G-Cloud 13**

### **Service Definition**

Everbridge Critical Event Management Suite

### **Lot 2 Cloud Software**

## Contents

<b>1.     <i>Introduction</i></b>	<b>3</b>
<b>Company Overview .....</b>	<b>3</b>
<b>Value Proposition .....</b>	<b>3</b>
<b>Social Value .....</b>	<b>3</b>
<b>Overview of the G-Cloud Service.....</b>	<b>4</b>
Mass Notification	4
CareCoverge for NHS	5
Safety Connection	5
Digital Operations	6
Crisis Management	6
<b>2.     <i>Data Protection</i></b>	<b>7</b>
<b>Information Assurance .....</b>	<b>7</b>
<b>Data Back-Up, Data Restoration and Disaster Recovery .....</b>	<b>7</b>
Data processing & storage location	7
Data restoration / service migration	8
Back Up & restore	8
Business continuity statement/plan	8
<b>Privacy by Design.....</b>	<b>9</b>
<b>3.     <i>Using the service</i></b>	<b>10</b>
<b>Ordering and Invoicing .....</b>	<b>10</b>
<b>Pricing Overview.....</b>	<b>10</b>
<b>Availability of Trial Service .....</b>	<b>10</b>
<b>On-Boarding, Off-Boarding, Service Migration, Scope etc.....</b>	<b>10</b>
<b>Training.....</b>	<b>11</b>
<b>Implementation Plan.....</b>	<b>11</b>
<b>Service Management.....</b>	<b>12</b>
<b>Service Levels.....</b>	<b>12</b>
<b>Outage and Maintenance Management .....</b>	<b>13</b>
<b>4.     <i>Provision of the service</i></b>	<b>15</b>
<b>Customer responsibilities.....</b>	<b>15</b>
<b>Technical Requirements and Client-Side Requirements.....</b>	<b>15</b>
<b>Outcomes/Deliverables.....</b>	<b>15</b>
<b>Development life cycle of the solution.....</b>	<b>15</b>
<b>After-sales Account Management.....</b>	<b>16</b>
<b>Termination Process .....</b>	<b>17</b>

5.     ***Our experience***

Clients .....

Contact details .....

18

18

18

# 1. Introduction

## Company Overview

Everbridge provides mass notification and interactive communication solutions that help business organisations increase connectivity to staff, clients, and other stakeholders while mitigating the impact of incidents on their most important assets and meeting data protection regulations for domestic and international operations.

## Value Proposition

Everbridge (NASDAQ: EVBG) is the global leader for integrated critical event management solutions that automate and accelerate organisations' operational response to critical events to help keep people safe and businesses running faster. Through its expertise in managing the complexity and unpredictability of critical events and unified critical communications, Everbridge ensures business, government and healthcare organisations are prepared to rapidly respond to - and even avoid - sudden, unexpected disruptions assisting with the critical event life cycle. 6,000 global organisations rely on the Everbridge Critical Event Management Platform to deliver organisational resilience on an unprecedented scale.

## Social Value

Everbridge is committed to providing social value within the following themes of PPN 06/20

### Fighting Climate Change:

Climate Change is driving a huge increase in extreme weather and natural disasters globally. Everbridge is providing data-driven indicators and software communications to unlock community & organisational resilience by helping to identify risk at a hyper-local level, warn people of extreme climate threats, and reduce loss and damage to governments and business. Everbridge supports the United Nations Sustainable Development Goal 13 and 17 by bridging the last mile of the Hydromet chain for public safety organisations, aiding the international organisation's efforts to ensure that 'by 2025 all countries have the capability for effective, authoritative emergency alerting.' Everbridge endorsed the collective efforts of the International Federation Of Red Cross And Red Crescent Societies (IFRC), International Telecommunication Union (ITU) and World Meteorological Organisation (WMO) as part of the Call to Action on Emergency Alerting.

### Covid 19 Recovery:

Everbridge provides technology led solutions to enable organisations to return safely to the workplace by:

- Surveying employees to assess their health and needs
- Conducting regular wellness checks

- Determining employee's readiness for returning to work

The Everbridge platform provides:

End-to-end Contact Tracing for an organisations people anywhere they might be at any point in time, with end-to-end Contact Tracing capabilities which includes current, past and expected locations, potential exposure, and follow-up management. Should they be:

- In your company's facilities and buildings (via integration with building access system, Wi-Fi hotspots, facility security equipment, and more)



- Moving between buildings or campuses
- Working remotely via GPS localization or self check-in
- Travelling (via integration with your travel itinerary systems)

Capturing location data from different sources in addition to proximity data, while fully adhering to privacy regulations and restrictions, constitutes the richest information that helps you understand the potential exposure of your employees and therefore take appropriate actions.

### **Equal Opportunity:**

We prioritise diversity, equity and inclusion to create a workplace that reflects the customers and populations we serve. We demonstrate our commitment to DEI by focusing on several key initiatives. This includes aligning our hiring and recruiting practices to attract a diverse and talented workforce; creating employee resource groups dedicated to celebrating and empowering communities within our organisation, including women, employees of colour, employees who identify as LGBTQ+, and members of the military and first responders; holding open forums for company-wide discussion and dialogue on civil unrest and equal justice; and supporting a growing ecosystem of minority-owned and led suppliers and partners.

## **Overview of the G-Cloud Service**

Everbridge provides a unified critical communications suite of applications that enable organisations to manage the entire critical event lifecycle. The suite has been designed to be used either as a single application for specific critical plans, mass communications & incidents, or in combination to manage multiple or all parts of the process.

The suite is used by both private and public sector customers including: Central Government Departments, Local Authorities, Emergency Services and NHS Trusts.

The applications within the suite are:

- **Mass Notification**
  - **CareConverge for NHS**
  - **Safety Connection**
  - **Digital Operations**
  - **Crisis Management**

### **Mass Notification**

Enables organisations to send mass notifications via SMS, Email, Voice, Mobile App & more than 20 other contact paths to individuals or groups using lists, locations, and visual intelligence. The application keeps your contacts informed before, during and after all events operational incidents, and emergencies, it also enables organisations to automate critical communications workflow according to pre-configured roles, rules and templates and executed with one simple click.

- Target individuals, groups, or use dynamic rules to reach the right people.
- Target key stakeholders to join instant conference calls with no pre-booking
- Mass Notification features robust analytics, GIS capabilities, and flexible contact management.
- Simple workflow that prompts users to select the correct incident type, before one click sending.
- User prompts for critical details to any communication using customizable fields

created by Incident Administrators

- Simple one click sending from desktop or mobile application
- Incident journal for post event reporting and audit

## CareCoverge for NHS

Everbridge enables NHS Hospitals to coordinate multiple clinicians, technicians, and staff across multiple locations and schedules to respond to clinical and operational events efficiently and effectively leading to increase response times, quality and patient satisfaction.

Everbridge aggregates multiple communication paths to send 2-way communications via SMS, Email, Voice, Mobile App & On-screen notifications to individuals or groups by role type and or location.

The application keeps stakeholders informed before, during and after all events, operational incidents, and emergencies, it also enables organisations to automate communications workflow according to pre-configured roles, rules and templates and executed with one simple click.

The application is used by multiple Acute, Foundation and University NHS Trusts in the UK and more than 800 acute care hospitals globally.

Everbridge provides:

- Simple workflow to reduce total communication time to under 1 minute, saving time in critical events such a 2222 call or a major incident.
- NHS specific pre built templates for events like cardiac arrest, stroke, mass casualty, missing patient, IT outage, fire, lock down, bed capacity checks etc.
- 2-way communication paths with confirmation receipt, polling questions or smart conference bridges. Enabling NHS trusts to track responses in real time and show who has received the message with a data and time stamp
- Target individuals, groups, using dynamic rules such as schedules, rotas, locations and skill set to reach the right people, via a simple one click send from a mobile application or desktop.
- Clinical Messaging - In built secure Clinical messaging app to provide a secure and governable 'WhatsApp' replacement. Providing Text, Voice, Video Calling, Message Groups and Photos. All of which are fully auditable.
- Open API's for the adoption of links with external 3<sup>rd</sup> party solutions
- Analytics to provide full reporting and audit trail

## Safety Connection

Safety Connection helps organisations quickly locate and communicate with their mobile employees. The solution aggregates geo-location data from multiple systems so that you can reach out to those who are potentially at risk at a specific scene.

- Interact with people using 2-way communication and send-receive pictures.
- The 3-in-1 Panic Button app available on iOS and Android
- Automatically keep employee locations current even when they are travelling or moving between buildings and campuses. Automatic acquisition of location data from:
  - Access control and badging systems
  - Wired and wireless network access points

- Hoteling systems
- Travel management system

## Digital Operations

Provides organisations with the ability to accelerate on-call staff response to unplanned IT issues and restore services within their service level agreements. Calendar and shift management keep staff on-call schedules up to date and automatically determine who's on-call (primary and backup), and who to escalate to should that be needed.

- '1-click' conferencing capability means people can quickly jump on a team call. No number to memorise or dial, no access code to enter; get automatically connected to the conference from a voice message, a SMS or an email from anywhere in the world. Incident managers can also easily decline callers or mute participants.
- Quickly access detailed reports and audit trails. Know instantly who was contacted, via which communication channel, as well as who responded, and at what time.

## Crisis Management

Everbridge Crisis Management provides organisations a single solution for business continuity, disaster recovery and emergency communication. In one application, crisis teams can coordinate all response activities, teams and resources to accelerate recovery times and maintain command and control when crises evolve into unanticipated scenarios.

With all stakeholders – from responders in the field to executives in the boardroom – working from a common operating picture, you will never have to worry that your response plans are not getting executed or tear yourself away from mission critical activities to provide a status update.

Fully integrated with the Everbridge Critical Event Management Platform, Crisis Management employs Everbridge's best-in-class technology for mass notification, incident management and mobile collaboration.

### **Unified Response and Communication**

Crisis Management orchestrates all crisis response activities, teams, resources and communications from a single event page, Includes operator dashboards, integrated chat, incident log and smart conferencing.

### **Dynamic Task Management**

The Crisis Management Task Manager helps turn static SOPs into actionable tasks that can be assigned to an individual, a group or a function. Tasks can be added on-the-fly in the middle of a crisis when unanticipated situations and scenarios arise. Everbridge Crisis Management Maintain Command and Control.

### **Mobile Response Plans**

Crisis Management allows users to mobilise response teams, execute plans (BC/DR, Emergency), and collaborate with team members no matter device or where they are located.

### **Executive View and Reporting**

Dedicated event dashboards and situation reports allow senior management to monitor response

and  
recovery progress in real-time without having to disrupt the crisis team.

## 2. Data Protection

### Information Assurance

Everbridge is an ISO27001, ISO 27701, SOC2, SOC3, FISMA, Safety Act, EU-US Privacy Shield, G-Cloud, and UK ICO certified organisation and we have achieved FedRAMP “In Process” status. Our security policies are governed by NIST 800-53, Controls for Moderate Impact systems, and an overview of our security policies and attestations can be found on the Everbridge Website, our security attestations are reviewed and updated annually.

### Data Back-Up, Data Restoration and Disaster Recovery

Everbridge’s system is designed to provide a true zero point of failure system. We employ multiple data centres for all of our test and production systems in a fully redundant, geographically dispersed configuration.

Data is continuously replicated between the various sites, and each site can provide the full range of Everbridge services. If service is disrupted at any site, all traffic is dynamically re-routed to another site so that Everbridge's systems remain constantly available. This transition is invisible to the client, who experiences no downtime as a result. Every system and tier within the Everbridge infrastructure is individually fault tolerant, with redundant power, networking, and hardware, telephony, and data communication wherever possible. The shared SaaS architecture methodology enables Everbridge to be available to our clients at 99.99% or greater.

All support and technical operations are conducted from within the Everbridge corporate office locations in Pasadena, CA, Burlington, MA, and Colchester, UK. Everbridge maintains up to date BCDR plans which include “rolling” support services throughout the globe should a catastrophic event strike one or more of our corporate office locations.

All notification platform services are hosted in SOC 2 facilities. These facilities are fully redundant, and Everbridge leverages a shared SaaS design allowing both data centres to simultaneously support all clients while providing full geographic fault-tolerance.

Should a catastrophic event occur, and the recovery of systems is required, the maximum Recovery Time Objective (RTO) is 15 minutes (or less) and the Recovery Point Objective (RPO) is 24 hours (or less).

### Data processing & storage location

Everbridge maintains several implementations in which clients may choose to store data which regardless of data store, is encrypted “at rest”.

#### **Today, these implementations include:**

- United Kingdom (London)
- Germany (Berlin)
- The Netherlands (Amsterdam)

- United States (Burbank, CA; Denver, CO; private cloud)
- Canada (Toronto, private cloud)

Data is not replicated from international environments (UK, Germany, Canada) to the United States at any time. In addition, each data store location contains multiple



geographically dispersed data centres which provide fault tolerance for any region while maintaining data privacy and adhering to international regulations.

## Data restoration / service migration

Everbridge communicates maintenance activities, service degradation events, and system status alerts via service advisories posted on the Everbridge Support Centre. Service advisories are available for thirty days beyond the conclusion of the maintenance or event. If a Customer would like to be notified of service advisories as they are posted, a Customer can configure service advisory notifications.

Everbridge is committed to maintaining the highest levels of performance and availability of the solution and there are occasions, however, when the service may be interrupted for planned or event-driven maintenance. Defined below are the different categories of solution maintenance and the standard maintenance windows and advisory periods.

- **PLANNED MAINTENANCE** - Any maintenance activity with an anticipated impact to system performance, availability, or functionality is considered.
- **UNPLANNED MAINTENANCE** - In order to prevent or mitigate potential service degradation, we may occasionally need to conduct maintenance without being able to provide an advance notification.
- **EMERGENCY MAINTENANCE** - If a service degradation does impact the Everbridge solution, our first priority is to restore service and resume normal operation. Under such circumstances, we may need to perform restorative maintenance.

## Back Up & restore

Everbridge's system is designed to provide a true zero-point-of-failure system. To provide the unique architecture, Everbridge employs multiple data centre locations in each of our production implementations across the UK, Europe and the US. Data is continuously replicated between each data centre location within a specific production implementation, and each data centre site can provide the full range of Everbridge services. If service is disrupted at either data centre, all traffic is dynamically rerouted to the remaining data centres so that Everbridge's systems remain constantly available to all of our clients.

Each data centre site is designed with full redundancy from top to bottom. Dual network up-links feed dual routers, fully meshed with dual load balancers, which secure the front-end network with tight controls. Each tier of servers is clustered using a combination of highly customised, secure, high performing, and scalable database solutions, which allows for real-time load balancing and failover between nodes, and affords easy scalability to meet increasing demand.

Everbridge's commits to service availability of 99.99% or greater, measured on a calendar quarterly basis including scheduled maintenance windows.

## Business continuity statement/plan

Everbridge has a Business Continuity – Disaster Recovery plan in place that is tested once per year. Recovery efforts strive to resume all business activities as soon as possible and

many recovery tasks will be conducted in tandem. However, in the event that prioritisation is necessary, Everbridge has established a recovery order for all business areas of the company. Everbridge has recovery plans for different types of disruptions: natural disasters, accidents or failures, technical disasters, or malicious activities.

Everbridge maintains up-to-date BCDR plans which include “rolling” support services throughout the globe should a catastrophic event strike one or more of our corporate office locations. Everbridge Technical Support uses a “follow the sun” policy such that technical support is based in multiple time zones in the US and abroad. A client’s support case may be addressed by non-US Everbridge personnel if support is sought during non-business hours in the US. We offer Technical Support from any of US, UK, Norway, China, and India locations.

Everbridge employs multiple data centres for all its test and production systems in a fully redundant, geographically dispersed configuration. Data is continuously replicated between the various sites, and each site can provide the full range of Everbridge services. If service is disrupted at any site, all traffic is dynamically rerouted to another site so that Everbridge’s systems remain constantly available. Every system in the infrastructure is individually fault tolerant, with redundant power, network, and disc, wherever possible.

Should a catastrophic event occur, and the recovery of systems is required, the maximum Recovery Time Objective (RTO) is 15 minutes (or less) and the Recovery Point Objective (RPO) is 24 hours (or less).

Upon final selection and under NDA, Everbridge can also provide our BCDR Plan Table of Contents and our latest Continuity Plan Test Results for further review.

## Privacy by Design

Recognising the sensitivity of the customer data to which Everbridge may have access, data privacy has long been an area of focus for us. First and foremost, any data processing performed by Everbridge is done at the initiative of our customers when they are utilising our system for critical events management. Everbridge does not process customer data in any other way or for any other reason. Second, customers have complete control over the data which is uploaded into Everbridge’s contact stores.

Everbridge does not access that data except as specifically requested by a customer, and all such data can be deleted or modified by a customer directly at any time. Upon expiration of a customer relationship, all customer data is deleted within 30 days. This control over the data enables customers to directly upload, modify and delete individual contact information as appropriate based on customer requirements. Everbridge’s systems will not need to be modified to comply with these key aspects of GDPR – the rights of individuals to view and correct their information and the “right to be forgotten.”

Everbridge’s security framework is based on National Institute of Standards and Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Information (maps to ISO 27001), and our security and data privacy controls and procedures are assessed annually by accredited third party audit firm under Statement on Standards for Attestation Engagements No. 16 (SSAE 18).

Finally, Everbridge is certified under the EU-US Privacy Shield and complies with its 7 principles: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

## 3. Using the service

### Ordering and Invoicing

A PO and signed call off order is required to initiate the service as per the Digital Marketplace. Invoice - net 30 days following submission of a valid invoice quoting a current purchase order.

### Pricing Overview

- All pricing is per contract year
- Invoicing is annual in advance with net 30-day payment terms
- All pricing excludes VAT
- Minimum order value of [REDACTED]
- Mass Notification & Safety Connection are priced based upon the number of recipient contacts
- Capabilities of Standard & Pro Mass Notification, Safety Connection & IT Alerting are shown in the pricing document
- Remote implementation, set up and training is [REDACTED] of the first year Suite and options price.
- Premium implementation and training is available via the Everbridge SFIA Rate Card
- Optional services are available as shown in the pricing table
- Minimum Contract Term is 12 Months
- Early termination will incur a fee

### Availability of Trial Service

Everbridge can provide customers with a pilot or proof of concept environment based on their specific requirements. Everbridge staff will work with the customer to identify a clear set of success criteria in order to achieve a successful outcome. Highly trained staff will guide the customer through the process and ensure they have sufficient knowledge and understanding to deliver the requirements.

### On-Boarding, Off-Boarding, Service Migration, Scope etc.

Everbridge provides customers with access to a dedicated implementation and Professional Services team to guide them through a pre-defined and well tested process to achieve success. Dependant on the project scale, this may involve multiple Everbridge staff from different disciplines working with the customer's stakeholder team.

A standard on-boarding process will provide the following:

- Orientation to your on-boarding resources, including the Everbridge Client Portal, knowledgebase articles library, and Everbridge University.
- Access to your functional account, configured with default templates and default notification paths. Everbridge provides a combination of remote and on-site on-boarding services tailored to the customer's requirement and need which includes on-site training,

online e-learning and user documentation 30-minute hands-on demo of creating new users, the basic setup of contacts and the sending of a test notification.

- Best practices and on-boarding guidance.

Everbridge does not assume ownership of any client data uploaded into the Everbridge system. If the client and Everbridge choose to end their agreement with each other, the client will be able to download all contact information stored in the Everbridge system and use it how it wishes.

When an organisation's contract expires, the organisation's account will be deactivated and listed for deletion. Thirty-days from the contract expiration date, the organisation's data will be flagged for purging and all of the organisation's data will be removed from the active system. Everbridge retains the organisation's data for one month in the event the organisation wishes to extend its subscription.

Upon any termination of this Agreement, the Receiving Party shall continue to maintain the confidentiality of the Disclosing Party's Confidential Information and, upon request and to the extent practicable, destroy all materials containing such Confidential Information.

The Everbridge Professional Services team can provide customers with consultancy services, this can be to directly or indirectly support the on-boarding or off-boarding of the Everbridge platform.

## Training

Everbridge provides all customers with access to the Everbridge University, the always on-line e-learning platform with the following benefits:

- Are continuously available and free for customers to learn or review
- Online videos with audio narrations
- Self-paced training that allows students to learn when they have time and at their own pace
- Just-in-time learning using small, focused content modules
- No travel or facilities required; the classroom is anywhere a learner has Internet access

Everbridge can also provide customers with a bespoke and tailored training program delivered by the Everbridge Professional Services team either on-site with the customer or remotely.

All of this is supported by the online user guide and 24/7/365 technical support team.

## Implementation Plan

Because Everbridge products are offered on-demand as a service over the Internet and telephone, no hardware or software installation is required, and the implementation life cycle for

our products is designed to enable your organisation to benefit quickly from the use of Everbridge.

Everbridge system implementations are a critical strength of our company, and our

implementation milestones are straightforward and simple. The Everbridge Client Services Implementation team is typically able to get clients fully deployed within 10-15 days; however, this is dependent on your team's availability, and we will work with your project team to complete the implementation within the desired timeframe.

An Everbridge Implementation Specialist will be available to ensure the success of your project. Additionally, Everbridge will review and provide input on communication best practices, incorporating lessons we have learned over the past 18 years.

## Service Management

Everbridge is a SaaS-based unified critical communications solution enabling our clients to communicate very quickly with any number of desired recipients, targeting a variety of devices and modalities for contacting those individuals, from mobile apps that function when cell towers are overwhelmed, to traditional SMS, email, phone calls and other contact methods. Everbridge has been providing critical communication and incident management technology to the marketplace since 2002.

The Everbridge platform is hosted with full geographic redundancy, for all clients, in a "shared" SaaS solution. This means that all hardware, software and capacity related to the notification system are hosted and managed entirely by Everbridge and authorised Everbridge personnel only. The only requirement for web-based access to the system is to leverage an internet browser which supports HTTPS TLS 256-Bit encryption. Everbridge also provides other means of access to the system, such as via telephone, with our Live Operator dispatch and through mobile devices.

Due to the hosted nature of the system, all maintenance and upgrades are performed internally by authorised Everbridge personnel and at no charge to our clients. During maintenance and upgrade procedures, clients are not impacted adversely in any way.

Using Everbridge requires no more than an existing Windows or Mac PC workstation with a web browser that supports HTTPS TLS 1.2 256-Bit encryption. Clients are not required to purchase, install, or maintain any hardware, software, or capacity to leverage the Everbridge system.

## Service Levels

Everbridge provides the following Service Level Objectives to all of our clients:

- **Broadcast Availability:** Everbridge makes every effort to ensure Everbridge services are available to our clients with a Broadcast Availability of 99.99% or greater. "Broadcast Availability" includes the ability to access the Everbridge solution in conjunction with the ability to deploy notifications to one or more contact paths (devices) per recipient.
- **Broadcast Performance:** During a 60-minute period, Everbridge shall make a minimum number of notification attempts to the 1<sup>st</sup> contact path for all client



broadcasts, using the standard configuration, per the table below. Notification attempts do not include third party network delivery.

Notification Type	Standard Configuration	Minimum Number of Notification Attempts in 60 minutes
Push to Everbridge mobile app		
Voice		
SMS		
Email		
Minimum numbers above do not apply when a Client uses the broadcast delivery throttling feature or intervals between delivery methods.		

## Outage and Maintenance Management

Everbridge's SOC 2 data centre facilities are rated Tier IV with fully redundant systems for power, HVAC, fire suppression, etc., and are a multi-region cloud configuration with numerous advantages including separation of power grids. If an electrical outage occurs, all data centres have what is called "N+1" redundant power systems, which means they can lose all of their primary power and still operate purely on backup systems. Because these sites reside in key telecommunications hubs they are held to the highest standards for environmental and service availability, and have priority status with such downstream services as diesel re-suppliers, and should get re-fuelled by one of their multiple providers at the same time as hospitals.

Everbridge's system is designed to provide a true zero-point-of-failure system. Everbridge provides an uptime guarantee of 99.99%. Data is continuously replicated between each data centre location within a specific production implementation, and each data centre site can provide the full range of Everbridge services. If service is disrupted at either data centre, all traffic is dynamically rerouted to the remaining data centre so that Everbridge's systems remain constantly available to all of our clients.

Everbridge monitors all aspects of the SaaS infrastructure from multiple points, both internal and external, using multiple tools and agents. The monitoring tools consist of host-based probes that are designed to detect any activity outside of normal application traffic. If a monitor detects any unusual or suspicious activity, then the monitoring tool generates an alert that is immediately investigated by our on-call support team. At each data centre, we have an intrusion-detection appliance which monitors all traffic on the back-end networks and borders watching for unusual or recognized traffic patterns. Furthermore, the appliances provide internal vulnerability scanning and external penetration testing tools which we use on a monthly basis to maintain a secure site. Should the on-call support team become aware of a security breach on the internal corporate or SaaS network, Everbridge is able to quickly disable any part or all of the infrastructure.

Should a catastrophic event occur, and the recovery of systems is required, the maximum Recovery Time Objective (RTO) is 15 minutes (or less) and the Recovery Point Objective (RPO) is 24 hours (or less).

Upon final selection and under NDA, Everbridge can also provide our Security Incident Response Policy and Plan for further review.

“Scheduled Maintenance” means maintenance scheduled in advance to implement updates and/or perform system maintenance. In general, the timing of Scheduled Maintenance will be posted at least two (2) business days prior to the Scheduled Maintenance window. However Scheduled Maintenance notifications may not be posted for all maintenance (particularly that which is not expected to impact customers). If Scheduled Maintenance is expected to interrupt Broadcast Availability, then a Scheduled Maintenance notification will be posted to the Client Services Portal and may be sent via email to all organisation leaders and account administrators

## 4. Provision of the service

### Customer responsibilities

The Customer shall retain all ownership rights in all Contact data and all electronic data the Client transmits to Everbridge to or through the Solution. The Customer also will represent that it has the right to authorise and hereby does authorise Everbridge to collect, store and process Customer data subject to the terms of the Agreement in the Digital Marketplace.

### Technical Requirements and Client-Side Requirements

Everbridge is a fully hosted SaaS solution and there are no requirements for our clients to install hardware, software, or manage capacity within their organisations. Requirements to access the solution via web browser include a browser that supports HTTPS TLS security. Access via mobile app will be via our Everbridge recipient app or ManageBridge. Access via telephone is through Phone Launch and/or Live Operator support.

Administrators will require an Internet enabled device whereas a recipient/user will require a mobile device that can receive any or all of the following SMS, Email, Voice or Data.

The supported languages that pronounce what is written in the body of the notification with the correct accent are as follows; English, French, German, Haitian creole, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish and Swedish.

#### **Browsers:**

A list of supported browsers includes Internet Explorer, Edge, Mozilla Firefox, Google Chrome, and Safari. These browsers have been tested on Windows and Mac. Everbridge supports any browser that can connect using 256-Bit TLS.

### Outcomes/Deliverables

Everbridge provides a web based Software as a Service Critical Event Management solution with ease-of-use as a priority, allowing users at all levels to quickly and easily send critical communications through the most intuitive user interface on the market allowing you to automate outreach via SMS, email, push notifications and more to communicate with employees and stakeholders in times of crisis, target messages to those impacted, or responsible for resolving issues and even allows you to communicate with those currently on a shift or employees who are scheduled to be on a shift in the future.

### Development life cycle of the solution

Everbridge utilizes the Agile development methodology, conducts all development of the notification platform internally, and maintains a formal system development lifecycle (SDLC) policy which includes application development, testing, security verification, and detailed change management procedures. These policies align to our security framework (governed by NIST

800-53 controls, FedRAMP, ISO 27001 compliance) and are in place to ensure secure development of application code and features, to test and verify all features developed, and to ensure smooth rollout to the Production environment without degrading our client's access or use of the platform.

We also develop the application with guidance from the following:

- ISO/IEC 27001 Information Security Management
- ISO/IEC 27002 Information Technology – Security Techniques (formerly ISO/IEC 17799)
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- NIST SP 800-122 to safeguard personally identifiable information,
- OWASP Top 10-2013: [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project#tab=OWASP\\_Top\\_10\\_for\\_2013](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013)
- Top 20 Critical Security Controls: <http://www.counciloncybersecurity.org/practice-areas/technology/>

## After-sales Account Management

From initial contact with an Account Executive to being fully implemented and beyond, Everbridge customers have access to a strong team of leaders with feet on the ground experience and years of expertise to assist you at every stage of the process.

- **Account Executive** – Your Account Executive is the individual who has developed a relationship with your organisation. He or she has acquired a strong product competency and industry knowledge related to market needs and domain knowledge specific to your industry. Furthermore, he or she has extensive experience understanding prospect customers' needs and advising on the best solution suite to meet and exceed their highest requirements. Everbridge Account Executives serve as your consultant and point-of-contact throughout the initial sales cycle and warmly introduce you to your Account Manager and Onboarding Specialist.
- **Onboarding Specialist** – Your Onboarding Specialist will provide professional onboarding, project management, and support resulting in a successful and well-coordinated implementation. During the process, your Onboarding Specialist will perform new client set up and system configuration, assist with data upload and management, and efficiently train new clients to use the application. He will also act as your escalation point and technical advocate within the company, providing quick and satisfactory resolution to all issues to ensure your satisfaction.
- **Account Manager** – Your Account Manager will take ownership of your account and immediately begin to develop a relationship that is meaningful and productive for your organisation. Account Managers have a minimum of three years of customer-focused experience. Your Account Manager will use that experience to develop a keen understanding of your business and service requirements in order to ensure Everbridge is always responsive to your needs. Account Managers also proactively review customer usage and service case activity to identify and mitigate potential service escalations. In addition, your Account Manager will share best practices and help you maximise the value of your purchased Everbridge products and services.
- **Implementation Specialist** – MSP's Implementation Specialist will provide professional implementation, project management, and support resulting in a successful and well-

coordinated implementation. During the implementation process, your Implementation Specialist will perform your set-up and system configuration, assist with data upload and management, and efficiently train your users to use the application. This specialist will also act as your escalation point and technical advocate within Everbridge, providing quick and satisfactory resolution to all issues so that we always ensure your satisfaction

## Termination Process

The customer acknowledges that it has purchased the Services for the Minimum Period will begin on the Effective Date and expire when all underlying Quotes with the Client have expired in accordance with the terms of such Quotes.

Either Party may terminate this Agreement upon the other Party's material breach of the Agreement, provided that (i) the non-breaching Party sends written notice to the breaching Party describing the breach in reasonable detail; (ii) the breaching Party does not cure the breach within thirty (30) days following its receipt of such notice (the "Notice Period"); and (iii) following the expiration of the Notice Period, the non-breaching Party sends a second written notice indicating its election to terminate this Agreement.

Early termination will incur a fee if not as a result of a material breach.



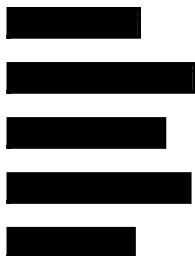
## 5. Our experience

### Clients



### Contact details

Everbridge



Phone: [REDACTED] [REDACTED]