



G-Cloud 13 Call-Off Contract

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

G-Cloud 13 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	12
Schedule 1: Services	36
Schedule 2: Call-Off Contract charges	40
Schedule 3: Collaboration agreement	42
Schedule 4: Alternative clauses	42
Schedule 5: Guarantee	42
Schedule 6: Glossary and interpretations	43
Schedule 7: GDPR Information	54

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.

Platform service ID number	483261797753165
Call-Off Contract reference	DDaT23305
Call-Off Contract title	DNS & Network Security Services
Call-Off Contract description	This Call Off Contract is for the provision of DNS hosting, unmetered DDoS mitigation and public network protection.
Start date	Friday 30 th June 2023
Expiry date	Monday 29 th June 2026
Call-Off Contract value	<p>The initial Call-Off Contract value for year 1 to year 3 for the Core Enterprise Plan shall not exceed [REDACTED] each year excluding VAT. Total Core Enterprise Plan cost for the 3 years shall not exceed [REDACTED]</p> <p>The value for a 12-month optional extension (year 4) shall not exceed [REDACTED] exclude VAT for the Core Enterprise Plan.</p> <p>There's also an option for the buyer to increase the scope of initial requirement during the term of the contract (3+1) to include additional services listed under Schedule 1- Services and the value shall not exceed [REDACTED] excluding VAT.</p> <p>The total maximum Call-Off contract value including any optional extensions shall not exceed \$ 1,153,907.92 excluding VAT for the 4 years. However, the Buyer is not committed to spend up to that amount.</p>
Charging method	BACS transfer
Purchase order number	To follow

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

Ref: DDaT23305

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.

From the Buyer	Innovate UK UK Research and Innovation Polaris House, N Star Ave, Swindon SN2 1FL
To the Supplier	Cloudflare, Inc, 101 Townsend Street San Francisco CA, 94107 USA [REDACTED]
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Head of Programme and Ops

Name: [REDACTED]

Email: [REDACTED]

For the Supplier:

Title: Account Executive - Public Sector

Name: [REDACTED]

Email: [REDACTED]

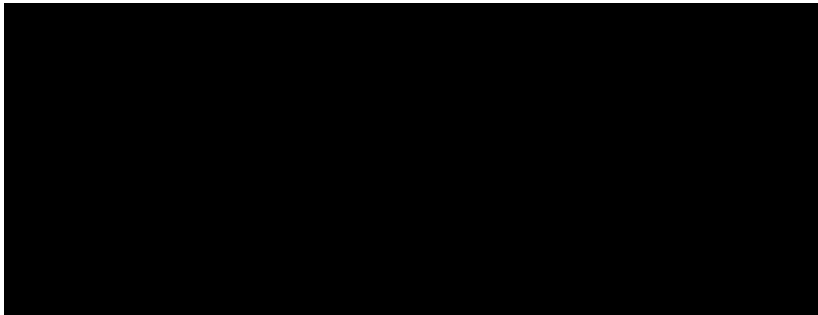
Phone: [REDACTED]

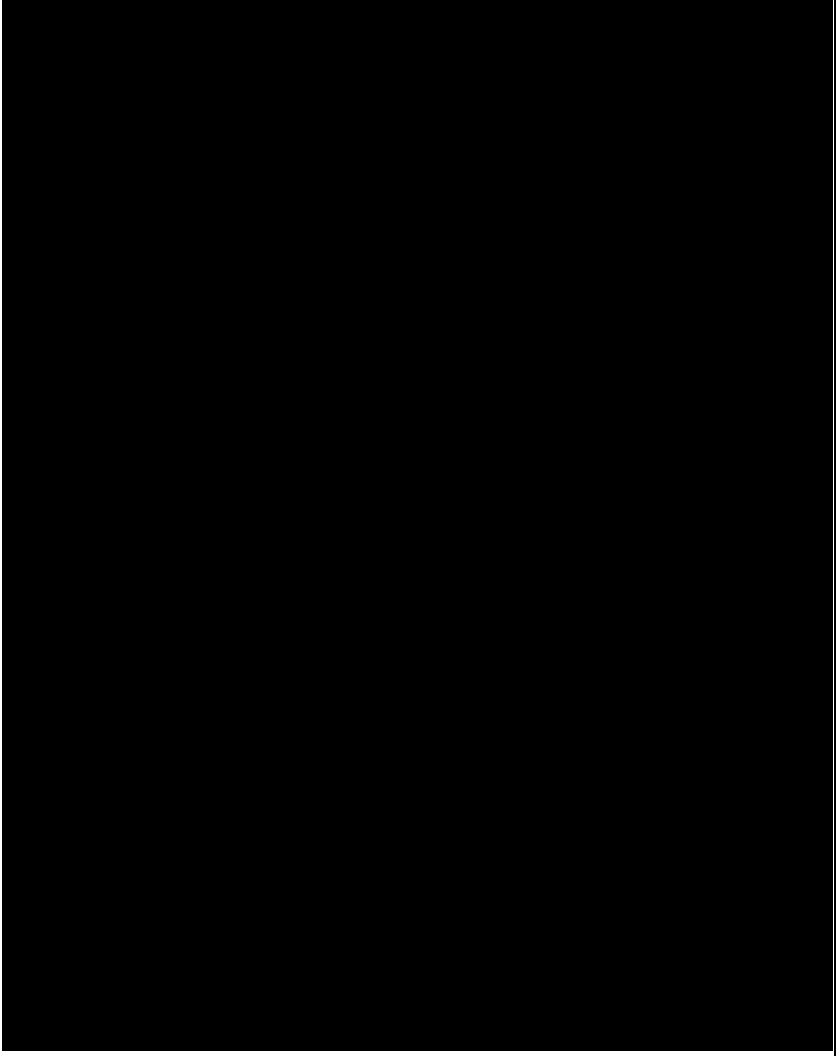
Call-Off Contract term

Start date	This Call-Off Contract Starts on Friday 30 th June 2023 and is valid for an initial period of 3 years till 29 th June 2026.
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	If required, this Call-Off Contract can be extended by the Buyer for one period of up to 12 months month from 30 th June 2026 to 29 th June 2027, by giving the Supplier 30 days written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.

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.

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 1: Cloud hosting
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> 

	
Additional Services	N/A
Location	N/A
Quality Standards	The quality standards required for this Call-Off Contract are in line with G-Cloud service offering and generally accepted industry practice.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are in line with G-Cloud service offering and generally accepted industry practice.

Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are:</p> <table border="1"> <thead> <tr> <th colspan="2">User support</th></tr> </thead> <tbody> <tr> <td>Email or online ticketing support</td><td>Email or online ticketing</td></tr> <tr> <td>Support response times</td><td>Phone, chat, and email support with median response time of 15 minutes critical business issues. Enterprise customers have access to our 24/7/3 emergency phone support hotline</td></tr> <tr> <td>User can manage status and priority of support tickets</td><td>Yes</td></tr> <tr> <td>Online ticketing support accessibility</td><td>None or don't know</td></tr> <tr> <td>Phone support</td><td>Yes</td></tr> <tr> <td>Phone support availability</td><td>24 hours, 7 days a week</td></tr> <tr> <td>Web chat support</td><td>Web chat</td></tr> <tr> <td>Web chat support availability</td><td>24 hours, 7 days a week</td></tr> <tr> <td>Web chat support accessibility standard</td><td>None or don't know</td></tr> <tr> <td>How the web chat support is accessible</td><td>N/A</td></tr> <tr> <td>Web chat accessibility testing</td><td>N/A</td></tr> <tr> <td>Onsite support</td><td>No</td></tr> <tr> <td>Support levels</td><td>Enterprise customers can choose between standard Enterprise support and Premium Support. Premium Enterprise support includes increased SLA response times and prioritised ticket handling. Standard Enterprise is included as a part of the standard Enterprise contract. Premium Support pricing is bespoke. Enterprise customers receive a dedicated Customer Success Manager and Solutions Engineer.</td></tr> </tbody> </table>	User support		Email or online ticketing support	Email or online ticketing	Support response times	Phone, chat, and email support with median response time of 15 minutes critical business issues. Enterprise customers have access to our 24/7/3 emergency phone support hotline	User can manage status and priority of support tickets	Yes	Online ticketing support accessibility	None or don't know	Phone support	Yes	Phone support availability	24 hours, 7 days a week	Web chat support	Web chat	Web chat support availability	24 hours, 7 days a week	Web chat support accessibility standard	None or don't know	How the web chat support is accessible	N/A	Web chat accessibility testing	N/A	Onsite support	No	Support levels	Enterprise customers can choose between standard Enterprise support and Premium Support. Premium Enterprise support includes increased SLA response times and prioritised ticket handling. Standard Enterprise is included as a part of the standard Enterprise contract. Premium Support pricing is bespoke. Enterprise customers receive a dedicated Customer Success Manager and Solutions Engineer.
User support																													
Email or online ticketing support	Email or online ticketing																												
Support response times	Phone, chat, and email support with median response time of 15 minutes critical business issues. Enterprise customers have access to our 24/7/3 emergency phone support hotline																												
User can manage status and priority of support tickets	Yes																												
Online ticketing support accessibility	None or don't know																												
Phone support	Yes																												
Phone support availability	24 hours, 7 days a week																												
Web chat support	Web chat																												
Web chat support availability	24 hours, 7 days a week																												
Web chat support accessibility standard	None or don't know																												
How the web chat support is accessible	N/A																												
Web chat accessibility testing	N/A																												
Onsite support	No																												
Support levels	Enterprise customers can choose between standard Enterprise support and Premium Support. Premium Enterprise support includes increased SLA response times and prioritised ticket handling. Standard Enterprise is included as a part of the standard Enterprise contract. Premium Support pricing is bespoke. Enterprise customers receive a dedicated Customer Success Manager and Solutions Engineer.																												
Onboarding	<p>The onboarding plan for this Call-Off Contract is:</p> <p>Cloudflare assists enterprise customers start using the service in a consultative manner using various methods, including remote and on-site and written documentation.</p>																												
Offboarding	<p>The offboarding plan for this Call-Off Contract is:</p> <p><u>End-of-contract data extraction</u></p> <p>The Cloudflare User Interface includes data aggregation logs, which include audit logs (log of every action taken within the interface and change to an account setting), as well as HTTP request logs. Data can be extracted via API in aggregate, or individual requests can be downloaded from the UI directly. Upon ending a contract, Cloudflare will advise customers on capturing all these data prior to account termination.</p> <p><u>End-of-contract process</u></p> <p>Cloudflare supports customers through the end of their contract and does not charge for reasonable off-boarding services. If a customer requires an extension of service during the off-boarding process, this may be subject to the same</p>																												

	terms as the original contract, but will be determined through joint agreement between Cloudflare and the buyer.
--	--

Collaboration agreement	N/A
Limit on Parties' liability	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £500,000 per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £500,000 excluding VAT during the Call-Off Contract Term.</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £500,000 excluding VAT during the Call-Off Contract Term.</p>
Insurance	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> • a minimum insurance period of 1 year following the expiration or Ending of this Call-Off Contract • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Buyer's responsibilities	The Buyer is responsible for providing all necessary information/assistance required by the Supplier in order to adequately provide the required supply.
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	N/A
-----------------------------------	-----

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.

Payment method	The payment method for this Call-Off Contract is BACS upon receipt of a valid invoice.
Payment profile	<p>The payment profile for this Call-Off Contract is:</p> <p>Payment shall be made Annually in advance, in USD, within 30 days upon receipt of an undisputed invoice</p>
Invoice details	<p>The Supplier will issue electronic invoices Annually, all invoices must quote a valid Purchase Order Number (PO Number)</p> <p>Payment of undisputed invoices will be made by the buyer within 30 days of receipt of an undisputed invoice, which must be submitted promptly by the Supplier.</p>
Who and where to send invoices to	<p>All invoices should be submitted in the Workday Supplier Porta, quoting a valid Purchase Order Number (PO Number), to:</p> <p>[REDACTED]</p> <p>Any query regarding an outstanding payment, please contact our finance team by email to: [REDACTED]</p>
Invoice information required	<p>All invoices must include a valid PO Number</p> <p>To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, item number (if applicable) and the details (name, email, and telephone number) of your Buyer contact (i.e. Buyer Authorised Representative). Non-compliant invoices may be sent back to you, which may lead to a delay in payment</p>

Invoice frequency	Invoice will be sent to the Buyer on annual basis
Call-Off Contract value	As set out under Part A: Order Form Call-Off Contract value
Call-Off Contract charges	The breakdown of the Charges is as per Schedule 3

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> • Access current DNS Setup (understand existing infrastructure) – 26/06/2023 - 30/06/2023 • Onboard third-party supplier and selected provider – 30/06/2023 • Add domain to DNS selected - 03/07/2023 – 04/07/2023 • Configuration (including IP addresses, CNAME, records, MX records for email server configuration etc) – 04/07/2023 – 11/07/2023 • Test DNS solution - 11/07/2023 – 14/07/2023 • Set TTL values – 17/07/2023 – 19/07/2023 • Update nameservers - 19/07/2023 – 21/07/2023 • Monitor DNS propagation – 24/07/2023 - 25/07/2023 • Validate DNS functionality - 25/07/2023 - 28/07/2023 • Monitor and manage DNS – from 28/07/2023
Guarantee	N/A
Warranties, representations	In line to the incorporated Framework Agreement clause 2.3
Supplemental requirements in addition to the Call-Off terms	N/A

Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Personal Data and Data Subjects	N/A
Intellectual Property	N/A
Social Value	<p>Fighting climate change</p> <p>Our goal is simple: help build a better, greener Internet with no carbon emissions that is powered by renewable energy. To help us get there, Cloudflare is making two announcements. The first is that we're committed to powering our network with 100% renewable energy. This builds on work we started back in 2018, and we think is clearly the right thing to do. We also believe it will ultimately lead to more efficient, more sustainable, and potentially cheaper products for our customers. The second is that by 2025 Cloudflare aims to remove all greenhouse gases emitted as the result of powering our network since our launch in 2010. As we continue to improve the way we track and mitigate our carbon footprint, we want to help the Internet begin with a fresh start. Finally, as part of our effort to track and mitigate our emissions, we're also releasing our first annual carbon emissions inventory report. The report will provide detail on exactly how we calculate our carbon emissions as well as our renewable energy purchases. Transparency is one of Cloudflare's core values. It's how we work to build trust with our customers in everything we do, and that includes our sustainability efforts.</p>

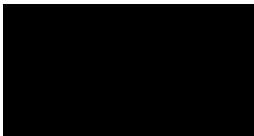
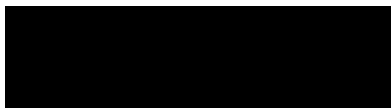
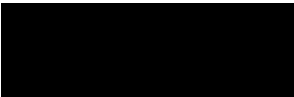

1. Formation of contract

- 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

Signed	Supplier (Cloudflare Ltd)	Buyer (UKRI)
Name		
Title	VP, Revenue Operations Vice President, Revenue Operations	Head of Procurement, UKSBS, DDaT
Signature		
Date	Jun 20, 2023	Jun 20, 2023

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

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 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)

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

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

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

3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

- 4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant

information needed to enable the Buyer to conduct its own IR35 Assessment.

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 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 £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause

34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party

shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

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

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off

Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

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

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

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

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud

Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject
(within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

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

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:

<https://www.gov.uk/government/publications/government-securityclassifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:

<https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive

Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk

management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN

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

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid

Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

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

18.2 The Parties agree that the:

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

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

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its

unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

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

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

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

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the

data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
 - 21.6.2 there will be no adverse impact on service continuity
 - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
 - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including

conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other

Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

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

Supplier's liability:

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

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

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 five million pounds (£5,000,000).

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.

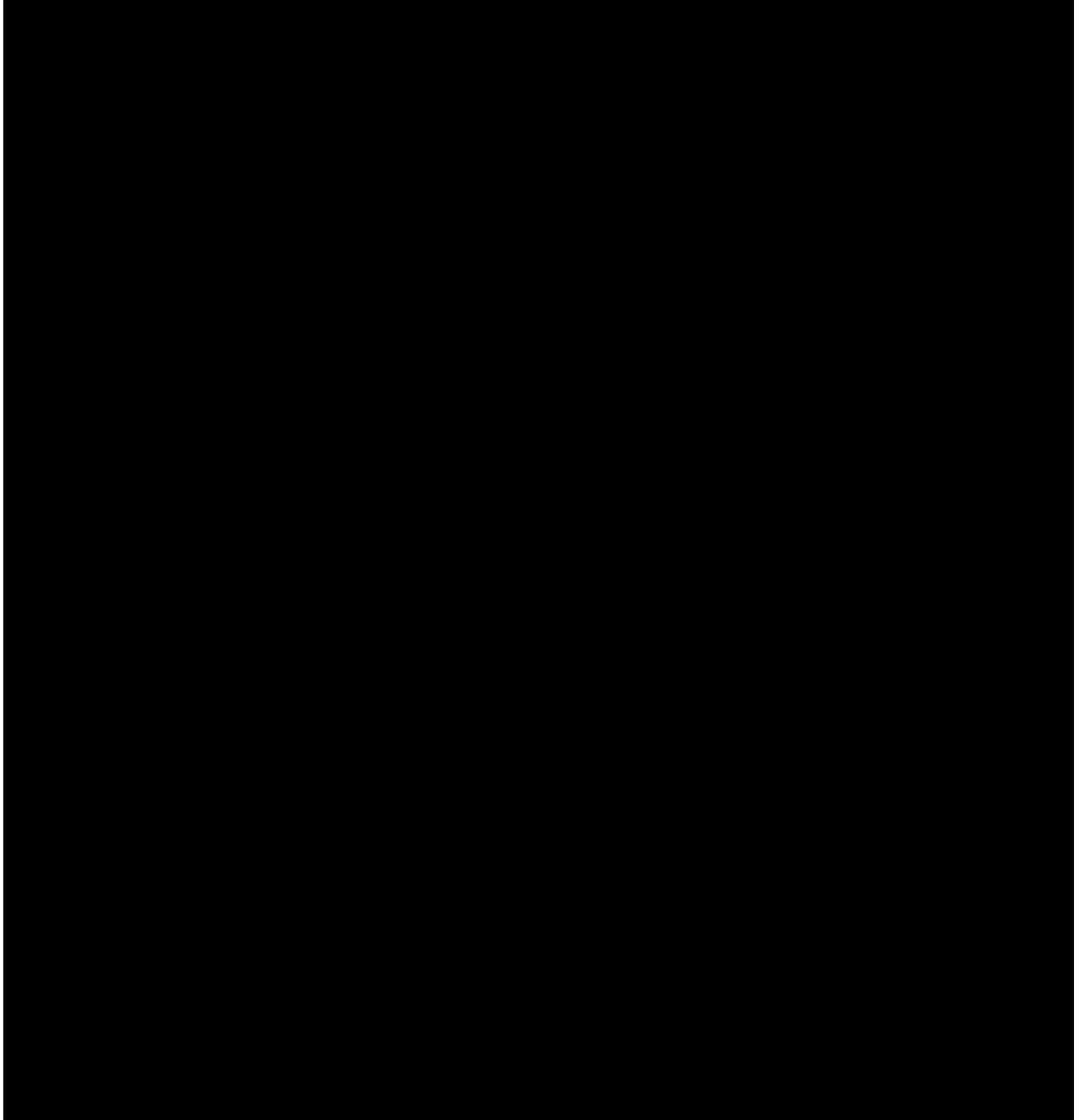
33. Data Protection Legislation (GDPR)

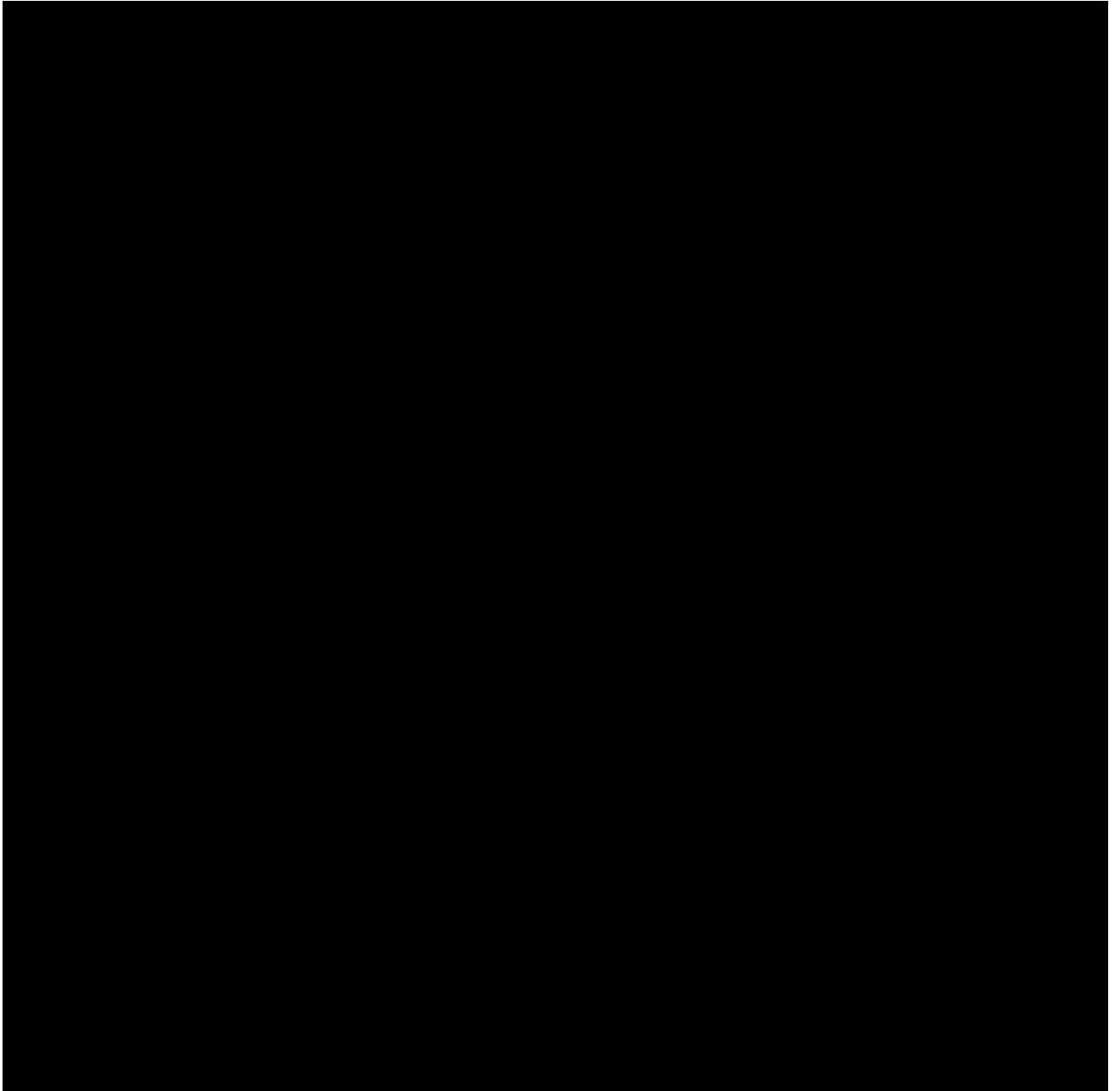
- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document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

Schedule 1: Services

Service to be provided is in line with supplier's G-Cloud service offering located and below:

Cloudflare Core Enterprise Plan incl. DNS Service





Asset protection

Knowledge of data storage and processing locations	Yes
Data storage and processing locations	<ul style="list-style-type: none"> • United Kingdom • European Economic Area (EEA) • Other locations
User control over data storage and processing locations	Yes
Datacentre security standards	Complies with a recognised standard (for example CSA CCM version 3.0)
Penetration testing frequency	At least once a year
Penetration testing approach	Another external penetration testing organisation
Protecting data at rest	<ul style="list-style-type: none"> • Physical access control, complying with CSA CCM v3.0 • Physical access control, complying with SSAE-16 / ISAE 3402 • Physical access control, complying with another standard • Encryption of all physical media • Scale, obfuscating techniques, or data storage sharding
Data sanitisation process	Yes
Data sanitisation type	Explicit overwriting of storage before reallocation
Equipment disposal approach	A third-party destruction service

Backup and recovery

Backup and recovery	Yes
What's backed up	Cloudflare conducts daily backups to maintain its service to customers
Backup controls	N/A - Cloudflare conducts backups to ensure restoration of customer accounts in the event of a complete data loss or disaster scenario within its primary data center. Cloudflare only has limited customer data and does not host its customers' websites, therefore customers do not control what is backed up or recovered.
Datacentre setup	Multiple datacentres with disaster recovery
Scheduling backups	Supplier controls the whole backup schedule
Backup recovery	Users contact the support team

Data-in-transit protection

Data protection between buyer and supplier networks	<ul style="list-style-type: none"> Private network or public sector network TLS (version 1.2 or above)
---	--

Data protection within supplier network	TLS (version 1.2 or above)
---	----------------------------

Availability and resilience

Guaranteed availability	100% uptime guarantee
-------------------------	-----------------------

Approach to resilience	<p>Cloudflare's network is based on Anycast routing, any one of thousands of servers in 270+ locations around the world is able to provide all of our service functionality on a given IP address. The network is the most interconnected network in the world - present in more Internet Exchanges globally than any other. The network is designed to cope with many nodes on the network map becoming unavailable and still providing service.</p> <p>Data centres are regularly taken offline for among other reasons maintenance without any service degradation. Should a certain location become unavailable due to high load from an attack, we will proactively re-route our prioritised Enterprise service level customers to ensure the minimal impact is seen for your application users in that region.</p> <p>Within each data centre, no single server/node is responsible for any service. These are also distributed across all metals such that server failures, hardware or networking issues won't impact the service/performance of our customers.</p>
------------------------	---

Outage reporting	Public dashboard, email alerts
------------------	--------------------------------

Identity and authentication

User authentication	<ul style="list-style-type: none"> 2-factor authentication Identity federation with existing provider (for example Google apps) Username or password
---------------------	---

Access restrictions in management interfaces and support channels	Cloudflare provides customer support through Zendesk, to which only the Cloudflare Support Team has access. Access to production is limited by role to the Systems Reliability Engineering team.
---	--

Access restriction testing frequency	At least every 6 months
--------------------------------------	-------------------------

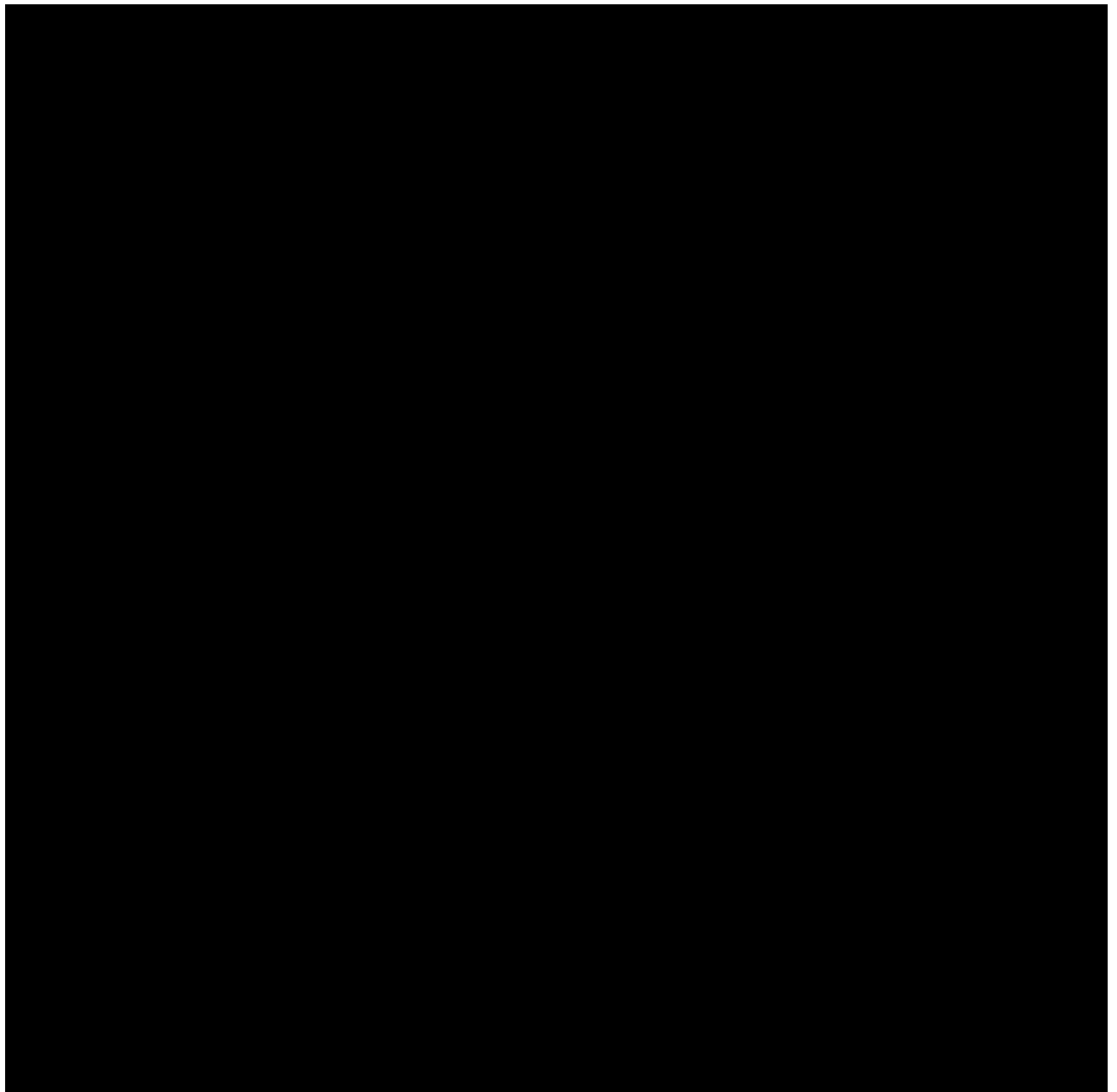
Management access authentication	<ul style="list-style-type: none"> 2-factor authentication Public key authentication (including by TLS client certificate) Identity federation with existing provider (for example Google Apps) Dedicated link (for example VPN) Username or password
----------------------------------	--

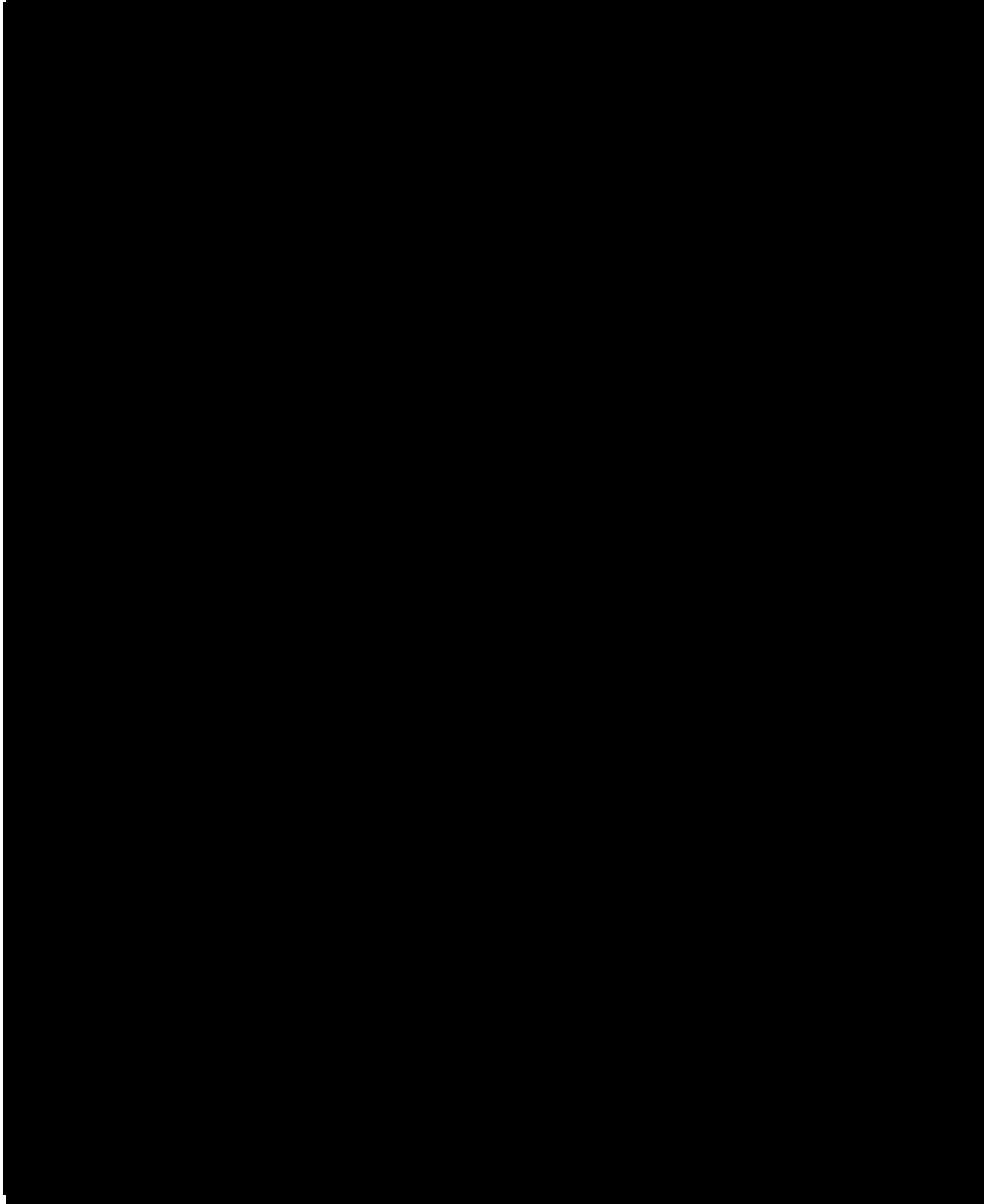
Devices users manage the service through	Directly from any device which may also be used for normal business (for example web browsing or viewing external email)
--	--

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:





Schedule 3: Collaboration agreement – Not Used

Schedule 4: Alternative clauses - Not Used

Schedule 5: Guarantee - Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> 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 created by the Party independently of this Call-Off Contract, or <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>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	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.
Call-Off Contract	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.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	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.
Commercially Sensitive Information	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.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> 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 other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	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.
Data Loss Event	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.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.

Data Protection Legislation (DPL)	(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.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • 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 <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>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	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.
Equipment	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.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	<p>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:</p> <p>https://www.gov.uk/guidance/check-employment-status-fortax</p>

Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<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"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • 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 • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • 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
Former Supplier	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).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	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.
Freedom of Information Act or FoIA	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.
G-Cloud Services	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.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	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.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	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.
Implementation Plan	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.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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 • 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 • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <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>
IPR claim	As set out in clause 11.5.
IR35	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.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	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.
Law	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.

Loss	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 ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	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.
Management Charge	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.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	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.
Ministry of Justice Code	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.

New Fair Deal	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.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.

Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	<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"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	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.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	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.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	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.
Relevant person	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.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	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.
Replacement supplier	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).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	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.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	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.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	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.
Subcontractor	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.
Sub processor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.

Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
--------------------------------	--

Supplier staff	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.
Supplier Terms	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.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1: Processing Personal Data

The Parties agree that the terms of the attached Data Processing Addendum will govern the data processing of any Personal Data (as defined in the DPA) by the Parties and forms part of the Framework Agreement.

Appendix 1

CLOUDFLARE DATA PROCESSING ADDENDUM

Cloudflare, Inc. (“**Cloudflare**”) and the counterparty agreeing to these terms (“**Customer**”) have entered into an Enterprise Subscription Agreement, Self-Serve Subscription Agreement or other written or electronic agreement for the Services provided by Cloudflare (the “**Main Agreement**”). This Data Processing Addendum, including the appendices (the “**DPA**”), forms part of the Main Agreement.

This DPA will be effective, and will replace and supersede any previously applicable terms relating to their subject matter (including any data processing amendment, agreement or addendum relating to the Services), from the date on which Customer signed or the parties otherwise agreed to this DPA (“**DPA Effective Date**”).

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

DATA PROCESSING TERMS

This DPA applies where Cloudflare processes Personal Data as a Processor (or sub-Processor as applicable) on behalf of Customer to provide the Services and such Personal Data is subject to Applicable Data Protection Laws (as defined below).

The parties have agreed to enter into this DPA in order to ensure that appropriate safeguards are in place to protect such Personal Data in accordance with Applicable Data Protection Laws. Accordingly, Cloudflare agrees to comply with the following provisions with respect to any Personal Data that it processes as a Processor (or sub-Processor as applicable) on behalf of Customer.

1. Definitions

1.1 The following definitions are used in this DPA:

- a) **“Adequate Country”** means a country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.
- b) **“Affiliate”** means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists).
- c) **“Applicable Data Protection Laws”** means all laws and regulations that are applicable to the processing of Personal Data under the Main Agreement, including European Data Protection Laws and the United States Data Protection Laws.
- d) **“Cloudflare Group”** means Cloudflare and any of its Affiliates.
- e) **“Controller”** means an entity that determines the purposes and means of the processing of Personal Data, and includes “controller,” “business,” or analogous term as defined under the Applicable Data Protection Laws.
- f) **“Customer Group”** means Customer and any of its Affiliates.
- g) **“European Data Protection Laws”** means all laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Main Agreement (including, where applicable, (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the **“EU GDPR”**); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (the **“UK GDPR”**); (iii) the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances (**“Swiss DPA”**); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv).
- h) **“Personal Data”** means all data which is defined as ‘*personal data*’, ‘*personal information*’, or ‘*personally identifiable information*’ (or analogous term) under Applicable Data Protection Laws.
- i) **“processing”, “data subject”, and “supervisory authority”** shall have the meanings ascribed to them in European Data Protection Law.
- j) **“Processor”** means an entity which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual’s personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data information for the purpose of providing the Services, and includes “processor,” “service provider,” or analogous term defined under the Applicable Data Protection Laws.
- k) **“Services”** shall refer to all of the cloud-based solutions offered, marketed or sold by Cloudflare or its authorized partners that are designed to increase the performance, security and availability of Internet properties, applications and networks, along with any software, software development kits and application programming interfaces (**“APIs”**) made available in connection with the foregoing.
- l) **“EU SCCs”** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
- m) **“Restricted Transfer”** means: (i) where the EU GDPR or Swiss Federal Act on Data Protection applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and

Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

- n) “**UK Addendum**” means the International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.
 - o) “**United States Data Protection Laws**” means all laws and regulations of the United States applicable to the processing of Personal Data under the Main Agreement, including (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations (collectively, the “CCPA”), (b) the Virginia Consumer Data Protection Act, when effective, (c) the Colorado Privacy Act and its implementing regulations, when effective, (d) the Utah Consumer Privacy Act, when effective; and (e) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring, when effective.
- 1.2 An entity “**Controls**” another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in “**Common Control**” if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.
- 1.3 For the purposes of this DPA, “to provide” or “providing” the Services means delivering the Services as defined in the Main Agreement;

2. Status of the parties

- 2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.
- 2.2 Each party warrants in relation to Personal Data that it will comply with and provide the same level of privacy protection as required by the Applicable Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.
- 2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that the Customer is the Controller (or a Processor processing Personal Data on behalf of a third-party Controller), and Cloudflare is a Processor (or sub-Processor, as applicable).
- 2.4 If Customer is a Processor, Customer warrants to Cloudflare that Customer’s instructions and actions with respect to the Personal Data, including its appointment of Cloudflare as another Processor and, where applicable, concluding the EU SCCs (including as they may be amended in clauses 6.2(b) and (c) below), have been (and will, for the duration of this DPA, continue to be) authorized by the relevant third-party Controller.

3. Cloudflare obligations

- 3.1 With respect to all Personal Data it processes in its role as a Processor or sub-Processor, Cloudflare warrants that it shall:
 - (a) only process Personal Data for the limited and specified business purpose of providing the Services and in accordance with: (i) the Customer's written instructions as set out in the Main Agreement and this DPA, unless required to do so by applicable Union or Member State law to which Cloudflare is subject, and (ii) the requirements of Applicable Data Protection Laws. In the event Cloudflare is required to process Personal Data under Applicable Data Protection Laws, Cloudflare shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) not use the Personal Data for the purposes of marketing or advertising;

- (c) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 2 (“**Security Measures**”). Customer acknowledges that the Security Measures are subject to technical progress and development and that Cloudflare may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service;
- (d) ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under contractual or statutory obligations of confidentiality;
- (e) without undue delay notify the Customer upon becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Cloudflare, its sub-Processors, or any other identified or unidentified third party (a “**Personal Data Breach**”) and provide the Customer with reasonable cooperation and assistance in respect of that Personal Data Breach, including all reasonable information in Cloudflare’s possession concerning such Personal Data Breach insofar as it affects the Personal Data;
- (f) not make any public announcement about a Personal Data Breach (a “**Breach Notice**”) without the prior written consent of the Customer, unless required by applicable law;
- (g) to the extent Cloudflare is able to verify that a data subject is associated with the Customer, promptly notify the Customer if it receives a request from a data subject to exercise any data protection rights (including rights of access, rectification or erasure) in respect of that data subject’s Personal Data (a “**Data Subject Request**”). Cloudflare shall not respond to a Data Subject Request without the Customer’s prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees;
- (h) to the extent Cloudflare is able, and in line with applicable law, provide reasonable assistance to Customer in responding to a data subject request to exercise any data protection rights under Applicable Data Protection Laws (including rights of access, rectification or erasure) in respect of that data subject’s Personal Data if the Customer does not have the ability to address a Data Subject Request without Cloudflare’s assistance. The Customer is responsible for verifying that the requestor is the data subject in respect of whose Personal Data the request is made. Cloudflare bears no responsibility for information provided in good faith to Customer in reliance on this subsection. Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance;
- (i) other than to the extent required to comply with applicable law, following termination or expiry of the Main Agreement or completion of the Service, at the choice of Customer, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA;
- (j) taking into account the nature of processing and the information available to Cloudflare, provide such assistance to the Customer as the Customer reasonably requests in relation to Cloudflare’s obligations under Applicable Data Protection Laws with respect to:
 - (i) data protection impact assessments and prior consultations (as such terms are defined in Applicable Data Protection Laws);
 - (ii) notifications to the supervisory authority under Applicable Data Protection Laws and/or communications to data subjects by the Customer in response to any Personal Data Breach; and
 - (iii) the Customer’s compliance with its obligations under Applicable Data Protection Laws with respect to the security of processing;

provided that the Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance; and

- (k) notify Customer if, in Cloudflare's opinion, any instructions provided by the Customer under clause 3.1(a) infringe Applicable Data Protection Laws, or if Cloudflare otherwise makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws
- 3.2 To the extent that Cloudflare is processing Personal Data on behalf of the Customer within the scope of the CCPA, Cloudflare makes the following additional commitments to Customer: Cloudflare will not retain, use, or disclose that Personal Data for any purposes other than the purposes set out in the Main Agreement and this DPA and as permitted under the CCPA, including under any "sale" exemption. Cloudflare will not "sell" or "share" such Personal Data, as those terms are defined in the CCPA. This clause 3.2 does not limit or reduce any data protection commitments Cloudflare makes to Customer in the Main Agreement or this DPA.
- 3.3 Cloudflare certifies that it understands and will comply with the obligations and restrictions in clauses 2 and 3, and the Applicable Data Protection Laws.

4. Sub-processing

- 4.1 Cloudflare will disclose Personal Data to sub-Processors only for the specific purpose of providing the Services.
- 4.2 Cloudflare will ensure that any sub-Processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-Processor terms (i.e., data protection obligations) that are no less protective of Personal Data than those imposed on Cloudflare in this DPA (the "**Relevant Terms**"). Cloudflare shall procure the performance by such sub-Processor of the Relevant Terms and shall be liable to the Customer for any breach by such sub-Processor of any of the Relevant Terms.
- 4.3 The Customer grants a general written authorization: (a) to Cloudflare to appoint other members of the Cloudflare Group as sub-Processors, and (b) to Cloudflare and other members of the Cloudflare Group to appoint third party data center operators, and business, engineering and customer support providers as sub-Processors to support the performance of the Service.
- 4.4 Cloudflare will maintain a list of sub-Processors at <https://www.cloudflare.com/gdpr/subprocessors/> and will add the names of new and replacement sub-Processors to the list at least thirty (30) days prior to the date on which those sub-Processors commence processing of Personal Data. If Customer objects to any new or replacement sub-Processor on reasonable grounds related to data protection, it shall notify Cloudflare of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If Cloudflare is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-Processor and decides in its discretion to do so, then Customer will have no further rights under this clause 4.4 in respect of the proposed use of the sub-Processor. If Cloudflare, in its discretion, requires use of the sub-Processor and is unable to satisfy Customer's objection regarding the proposed use of the new or replacement sub-Processor, then Customer may terminate the applicable Order Form effective upon the date Cloudflare begins use of such new or replacement sub-Processor solely with respect to the Service(s) that will use the proposed new sub-Processor for the processing of Personal Data. If Customer does not provide a timely objection to any new or replacement sub-Processor in accordance with this clause 4.4, Customer will be deemed to have consented to the sub-Processor and waived its right to object.

5. Audit and records

- 5.1 Cloudflare shall, in accordance with Applicable Data Protection Laws, make available to Customer such information in Cloudflare's possession or control as Customer may reasonably request with a view to demonstrating Cloudflare's compliance with the obligations of Processors under Applicable Data Protection Laws in relation to its processing of Personal Data.
- 5.2 Cloudflare may fulfill Customer's right of audit under Applicable Protection Laws in relation to Personal Data, by providing:
 - (a) an audit report not older than thirteen (13) months, prepared by an independent external auditor demonstrating that Cloudflare's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard;

- (b) additional information in Cloudflare's possession or control to a data protection supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Cloudflare under this DPA; and
- (c) To the extent that Customer's Personal Data is subject to the EU SCCs and the information made available pursuant to this clause 5.2 is insufficient, in Customer's reasonable judgment, to confirm Cloudflare's compliance with its obligations under this DPA or Applicable Data Protection Laws, then Cloudflare shall enable Customer to request one onsite audit per annual period during the Term (as defined in the Main Agreement) to verify Cloudflare's compliance with its obligations under this DPA in accordance with clause 5.3.

5.3 The following additional terms shall apply to audits the Customer requests:

- (a) Customer must send any requests for reviews of Cloudflare's audit reports to customer-compliance@cloudflare.com.
- (b) Following receipt by Cloudflare of a request for audit under clause 5.2(c), Cloudflare and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any audit under clause 5.2(c). Whenever possible, evidence for such an audit will be limited to the evidence collected for Cloudflare's most recent third-party audit.
- (c) Cloudflare may charge a fee (based on Cloudflare's reasonable costs) for any audit under clause 5.2(c). Cloudflare will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.
- (d) Cloudflare may object in writing to an auditor appointed by Customer to conduct any audit under clause 5.2(c) if the auditor is, in Cloudflare's reasonable opinion, not suitably qualified or independent, a competitor of Cloudflare, or otherwise manifestly unsuitable (i.e., an auditor whose engagement may have a harmful impact on Cloudflare's business comparable to the aforementioned aspects). Any such objection by Cloudflare will require Customer to appoint another auditor or conduct the audit itself. If the EU SCCs (including as they may be amended in clauses 6.2(a) and (b) below) applies, nothing in this clause 5.3 varies or modifies the EU SCCs nor affects any supervisory authority's or data subject's rights under the EU SCCs.

6. Data transfers from the EEA, Switzerland, and the UK

- 6.1 In connection with the Service, the parties anticipate that Cloudflare (and its sub-Processors) may process outside of the European Economic Area ("EEA"), Switzerland, and the United Kingdom, certain Personal Data protected by European Data Protection Laws in respect of which Customer or a member of the Customer Group may be a Controller (or Processor on behalf of a third-party Controller, as applicable).
- 6.2 The parties agree that when the transfer of Personal Data protected by European Data Protection Laws from Customer or any member of the Customer Group to Cloudflare is a Restricted Transfer then it shall be subject to the appropriate EU SCCs as follows:
 - (a) **EU Transfers:** in relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:
 - (i) Module Two will apply where Customer (or the relevant member of the Customer Group) is a Controller and Module Three will apply where Customer (or the relevant member of the Customer Group) is a Processor;
 - (ii) in Clause 7, the optional docking clause will apply;
 - (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in Clause 4.3 of this DPA;

- (iv) in Clause 11, the optional language will not apply;
 - (v) in Clause 17, Option 2 will apply, and if the data exporter's Member State does not allow for third-party beneficiary rights, then the law of Germany shall apply;
 - (vi) in Clause 18(b), disputes shall be resolved before the courts of the jurisdiction governing the Main Agreement between the parties or, if that jurisdiction is not an EU Member State, then the courts in Munich, Germany. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall fall on the country of the governing law;
 - (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and
 - (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA.
- (b) **UK Transfers:** in relation to Personal Data that is protected by the UK GDPR, the EU SCCs will apply as set out above in clause 6.2(a) of this DPA, shall apply to transfers of such Personal Data, except that:
- (i) The EU SCCs shall be deemed amended as specified by the UK Addendum, which shall be deemed executed between the transferring Customer (or the relevant member of the Customer Group) and Cloudflare;
 - (ii) Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum;
 - (iii) For the purposes of the UK Addendum, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA; and
 - (iv) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party."
- (c) **Swiss Transfers:** in relation to Personal Data that is protected by the Swiss Federal Act on Data Protection (as amended or replaced), the EU SCCs, completed as set out about in clause 6.2(a) of this DPA, shall apply to transfers of such Personal Data, except that:
- (i) the competent supervisory authority in respect of such Personal Data shall be the Swiss Federal Data Protection and Information Commissioner;
 - (ii) in Clause 17, the governing law shall be the laws of Switzerland;
 - (iii) references to "Member State(s)" in the EU SCCs shall be interpreted to refer to Switzerland, and data subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland; and
 - (iv) references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the EU SCCs shall be understood to be references to the Swiss Federal Act on Data Protection (as amended or replaced).
- (d) The following terms shall apply to the EU SCCs (including as they may be amended under clauses 6.2(b) and (c) above):
- (i) Customer may exercise its right of audit under the EU SCCs as set out in, and subject to the requirements of, clause 5 of this DPA; and

- (ii) Cloudflare may appoint sub-Processors as set out in, and subject to the requirements of, clauses 4 and 6.3 of this DPA, and Customer may exercise its right to object to sub-Processors under the EU SCCs in the manner set out in clause 4.3 of this DPA.
 - (e) In the event that any provision of this DPA contradicts, directly or indirectly, the EU SCCs (and the UK Addendum, as appropriate), the latter shall prevail.
- 6.3 In respect of Restricted Transfers made to Cloudflare under clause 6.2, Cloudflare shall not participate in (nor permit any sub-Processor to participate in) any further Restricted Transfers of Personal Data (whether as an “exporter” or an “importer” of the Personal Data) unless such further Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to EU SCCs implemented between the exporter and importer of the Personal Data or an Alternative Transfer Mechanism (as defined in clause 6.5) adopted by the importer applies.
- 6.4 In the event Customer seeks to conduct any assessment of the adequacy of the EU SCCs for transfers to any particular countries or regions, Cloudflare shall, to the extent it is able, provide reasonable assistance to Customer for the purpose of any such assessment, provided Customer shall cover all costs incurred by Cloudflare in connection with its provision of such assistance.
- 6.5 To the extent Cloudflare adopts an alternative data export mechanism (including any new version of or successor to the Privacy Shield adopted pursuant to applicable European Data Protection Laws) for the transfer of Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Personal Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect to such Alternative Transfer Mechanism.

7. Third Party Data Access Requests

- 7.1 If Cloudflare becomes aware of any third party legal process requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then Cloudflare will:
- (a) immediately notify Customer of the request unless such notification is legally prohibited;
 - (b) inform the third party that it is a Processor or sub-Processor (as applicable) of the Personal Data and is not authorized to disclose the Personal Data without Customer’s consent;
 - (c) disclose to the third party the minimum necessary Customer contact details to allow the third party to contact the Customer and instruct the third party to direct its data request to Customer; and
 - (d) to the extent Cloudflare provides access to or discloses Personal Data in response to third party legal process either with Customer authorization or due to a mandatory legal compulsion, then Cloudflare will disclose the minimum amount of Personal Data to the extent it is legally required to do so and in accordance with the applicable legal process.
- 7.2 In Cloudflare’s role as a Processor or sub-Processor, as applicable, it may be subject to third party legal process issued by a government authority (including a judicial authority) and requesting access to or disclosure of Personal Data. If Cloudflare becomes aware of any third party legal process issued by a government authority (including a judicial authority) requesting Personal Data that Cloudflare processes on behalf of Customer in its role as Processor or sub-Processor (as applicable) then, to the extent that Cloudflare reviews the request with reasonable efforts and as a result is able to identify that such third party legal process requesting Personal Data raises a conflict of law, Cloudflare will:
- (a) take all actions identified in clause 7.1 above;
 - (b) pursue legal remedies prior to producing Personal Data up to an appellate court level; and
 - (c) not disclose Personal Data until (and then only to the extent) required to do so under applicable procedural rules.

- 7.3 Clauses 7.1 and 7.2 shall not apply in the event that Cloudflare has a good-faith belief the government request is necessary due to an emergency involving the danger of death or serious physical injury to an individual. In such event, Cloudflare shall notify Customer of the data disclosure as soon as possible following the disclosure and provide Customer with full details of the same, unless such disclosure is legally prohibited.
- 7.4 Cloudflare will provide Customer with regular updates about third party legal process requesting Personal Data in the form of Cloudflare's semiannual Transparency Report, which is available at <https://www.cloudflare.com/transparency/>.
- 7.5 As of the date Customer entered into this DPA with Cloudflare, Cloudflare makes the commitments listed below. Cloudflare will update these commitments as may be required at <https://www.cloudflare.com/transparency/>:
- (a) Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.
 - (b) Cloudflare has never installed any law enforcement software or equipment anywhere on our network.
 - (c) Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.
 - (d) Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.

8. General


- 8.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.
- 8.2 Cloudflare's liability under or in connection with this DPA, including under the EU SCCs, is subject to the exclusions and limitations on liability contained in the Main Agreement. In no event does Cloudflare limit or exclude its liability towards data subjects or competent data protection authorities.
- 8.3 Except where and to the extent expressly provided in the EU SCCs or required as a matter of Applicable Data Protection Laws, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.
- 8.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws as specified in the Main Agreement, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts specified in the Main Agreement.
- 8.5 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable. Without limiting the generality of the foregoing, Customer agrees that clause 8.2 (Limitation of Liability) will remain in effect notwithstanding the unenforceability of any provision of this DPA.
- 8.6 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter.

Annex 1**Data Processing Description**


This Annex 1 forms part of the DPA and describes the processing that Cloudflare will perform on behalf of Customer.

A. LIST OF PARTIES


Data exporter(s): *Customer to complete the right-hand column.*

	Name: <i>Customer and any Customer Affiliates described in the Main Agreement.</i>	As stated in the Main Agreement
	Address: <i>Addresses of Customer and any Customer Affiliates described in the Main Agreement. (or otherwise notified by Customer to Cloudflare</i>	As stated in the Main Agreement
	Contact person's name, position and contact details:	
	Activities relevant to the data transferred under this DPA and the EU SCCs:	Use of the Service pursuant to the Main Agreement.
	Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
	Role (controller/processor):	Controller (or Processor on behalf of a third-party Controller).

Data importer(s):

	Name:	Cloudflare, Inc.
	Address:	101 Townsend Street San Francisco, CA 94107 USA
	Contact person's name, position and contact details:	

Ref: DDaT23305

		Data Protection Officer 
	Activities relevant to the data transferred under this DPA and the EU SCCs:	Processing necessary to provide the Service to Customer, pursuant to the Main Agreement.
	Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
	Role (controller/processor):	Processor (or sub-Processor)

B. DESCRIPTION OF DATA PROCESSING AND TRANSFER

Categories of data subjects whose Personal Data is transferred:	<p>Natural persons that (i) access or use Customer's domains, networks, websites, application programming interfaces ("APIs"), and applications, or (ii) Customers' employees, agents, or contractors who access or use the Services, such as Cloudflare Zero Trust end users, (together, "End Users").</p> <p>Natural persons with login credentials for a Cloudflare account and/or those who administer any of the Services for a Customer ("Administrators").</p>
Categories of Personal Data transferred:	<p>In relation to End Users:</p> <ul style="list-style-type: none"> Any Personal Data processed in Customer Logs, such as IP addresses, and in the case of Cloudflare Zero Trust, Cloudflare Zero Trust end user names and email addresses. "Customer Logs" means any logs of End Users' interactions with Customer's Internet Properties and the Service that are made available to Customer via the Service dashboard or other online interface during the Term by Cloudflare. Any Personal Data processed in Customer Content, the extent of which is determined and controlled by the Customer in its sole discretion. "Customer Content" means any files, software, scripts, multimedia images, graphics, audio, video, text, data, or other objects originating or transmitted from or processed by any Internet Properties owned, controlled or operated by Customer or uploaded by Customer through the Service, and routed to, passed through, processed and/or cached on or within, Cloudflare's network or otherwise

	<p>transmitted or routed using the Service by Customer.</p> <p>In relation to Administrative Users:</p> <ul style="list-style-type: none"> Any Personal Data processed in Administrative User audit logs, such as IP addresses and email addresses.
<p>Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:</p>	<p>Customer, its End Users, Administrators, and/or other partners may upload content to Customer's online properties which may include special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion.</p> <p>Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.</p> <p>Any such special categories of data shall be protected by applying the security measures described in Annex 2.</p>
<p>The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):</p>	<p>Continuous for the duration of the Main Agreement.</p>
<p>Nature of the processing:</p>	<p>Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Main Agreement and this DPA.</p>
<p>Purpose(s) of the data transfer and further processing:</p>	<p>Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Main Agreement and this DPA.</p>
<p>The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:</p>	<p>Until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable).</p>

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing:	The subject matter, nature and duration of the processing shall be as specified in the Main Agreement.
---	--

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 of the EU SCCs)	<p>In respect of the EU SCCs, means the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs.</p> <p>In respect of the UK Addendum, means the UK Information Commissioner's Office.</p>
---	---

Annex 2

Technical and Organizational Security Measures

Cloudflare has implemented and shall maintain an information security program in accordance with ISO/IEC 27000 standards. Cloudflare's security program shall include:

Measures of encryption of Personal Data

Cloudflare implements encryption to adequately protect Personal Data using:

- state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- trustworthy public-key certification authorities and infrastructure;
- effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Cloudflare enhances the security of processing systems and services in production environments by:

- employing a code review process to increase the security of the code used to provide the Services; and testing code and systems for vulnerabilities before and during use;
- maintaining an external bug bounty program;
- using checks to validate the integrity of encrypted data, and
- employing preventative and reactive intrusion detection.

Cloudflare deploys high-availability systems across geographically-distributed data centers.

Cloudflare implements input control measures to protect and maintain the confidentiality of Personal Data including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authenticating authorized personnel using unique authentication credentials (passwords) and hard tokens;
- automatically signing-out user IDs after a period of inactivity;
- protecting the input of data, as well as the reading, alteration and deletion of stored data; and
- requiring that data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked and secure.

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Cloudflare implements measures to ensure that Personal Data is protected from accidental destruction or loss, including by maintaining:

- disaster-recovery and business continuity plans and procedures;
- geographically-distributed data centers;
- redundant infrastructure, including power supplies and internet connectivity;
- backups stored at alternative sites and available for restore in case of failure of primary systems; and
- incident management procedures that are regularly tested.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Cloudflare's technical and organizational measures are regularly tested and evaluated by external third-party auditors as part of Cloudflare's Security & Privacy Compliance Program. These may include annual ISO/IEC 27001 audits; AICPA SOC 2 Type II; PCI DSS Level 1; and other external audits. Measures are also regularly tested by internal audits, as well as annual and targeted risk assessments.

Measures for user identification and authorization

Cloudflare implements effective measures for user authentication and privilege management by:

- applying a mandatory access control and authentication policy;

- applying a zero-trust model of identification and authorization;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- allocating and managing appropriate privileges according to role, approvals, and exception management; and
- applying the principle of least privilege access.

Measures for the protection of data during transmission

Cloudflare implements effective measures to protect Personal Data from being read, copied, altered or deleted by unauthorized parties during transmission, including by:

- using state-of-the-art transport encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as adequate firewalls, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms;
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;
- enforcing secure measures to reliably generate, manage, store and protect encryption keys; and
- audit logging, monitoring, and tracking data transmissions.

Measures for the protection of data during storage

Cloudflare implements effective measures to protect Personal Data during storage, controlling and limiting access to data processing systems, and by:

- using state-of-the-art encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- using trustworthy public-key certification authorities and infrastructure;
- testing systems storing data for software vulnerabilities and possible backdoors;
- employing effective encryption algorithms and parameterization, such as requiring all disks storing Personal Data to be encrypted with AES-XTS using a key length of 128-bits or longer.
- using correctly implemented and properly maintained software, covered under a vulnerability management program, and tested for conformity by auditing;
- enforcing secure measures to reliably generate, manage, store and protect encryption keys;
- identifying and authorizing systems and users with access to data processing systems;
- automatically signing-out users after a period of inactivity; and
- audit logging, monitoring, and tracking access to data processing and storage systems.

Cloudflare implements access controls to specific areas of data processing systems to ensure only authorized users are able to access the Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- applying a zero-trust model of user identification and authorization;
- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- monitoring actions of those authorized to delete, add or modify Personal Data;
- release data only to authorized persons, including the allocation of differentiated access rights and roles; and
- controlling access to data, with controlled and documented destruction of data.

Measures for ensuring physical security of locations at which Personal Data are processed

Cloudflare maintains and implements effective physical access control policies and measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers, and related hardware) where the Personal Data are processed or used, including by:

- establishing secure areas;
- protecting and restricting access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to data centers where Personal Data are hosted are logged, monitored, and tracked; and
- data centers where Personal Data are hosted are secured by security alarm systems, and other appropriate security measures.

Measures for ensuring events logging

Cloudflare has implemented a logging and monitoring program to log, monitor and track access to personal data, including by system administrators and to ensure data is processed in accordance with instructions received. This is accomplished by various measures, including:

- authenticating authorized personnel using unique authentication credentials and strong multi-factor authentication, including requiring the use of physical hard tokens;
- applying a zero-trust model of user identification and authorization;
- maintaining updated lists of system administrators' identification details;
- adopting measures to detect, assess, and respond to high-risk anomalies;
- keeping secure, accurate, and unmodified access logs to the processing infrastructure for twelve months; and
- testing the logging configuration, monitoring system, alerting and incident response process at least once annually.

Measures for ensuring system configuration, including default configuration

Cloudflare maintains configuration baselines for all systems supporting the production data processing environment, including third-party systems. Configuration baselines should align with industry best practices such as the Center for Internet Security (CIS) Level 1 benchmarks. Automated mechanisms must be used to enforce baseline configurations on production systems, and to prevent unauthorized

changes. Changes to baselines are limited to a small number of authorized Cloudflare personnel, and must follow change control processes. Changes must be auditable, and checked regularly to detect deviations from baseline configurations.

Cloudflare configures baselines for the information system using the principle of least

privilege. By default, access configurations are set to “deny-all,” and default passwords must be changed to meet Cloudflare’s policies prior to device installation on the Cloudflare network, or immediately after software or operating system installation. Systems are configured to synchronize system time clocks based on International Atomic Time or Coordinated Universal Time (UTC), and access to modify time data is restricted to authorized personnel.

Measures for internal IT and IT security governance and management

Cloudflare maintains internal policies on the acceptable use of IT systems and general information security. Cloudflare requires all employees to undertake general security and privacy awareness training at least every year. Cloudflare restricts and protects the processing of Personal Data, and has documented and implemented:

- a formal Information Security Management System (ISMS) in order to protect the confidentiality, integrity, authenticity, and availability of Cloudflare’s data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations; and
- a formal Privacy Information Management System (PIMS) in order to protect the confidentiality, integrity, authenticity, and availability of the policies and procedures supporting Cloudflare’s global managed network, as both a processor and a controller of customer information.

Cloudflare will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Cloudflare shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Annex 2.

Measures for certification/assurance of processes and products

The implementation of Cloudflare’s ISMS and related security risk management processes have been externally certified to the industry-standard ISO/IEC 27001. The implementation of Cloudflare’s comprehensive PIMS has been externally certified to the industry-standard ISO/IEC 27701, as both a processor and controller of customer information.

Cloudflare maintains PCI DSS Level 1 compliance for which Cloudflare is audited annually by a third-party Qualified Security Assessor. Cloudflare has undertaken other certifications such as the AICPA SOC 2 Type II certification in accordance with the AICPA Trust Service Criteria, and details of these and other

certifications that Cloudflare may undertake from time to time will be made available on Cloudflare's website.

For transfers to (sub-) Processors, also describe the specific technical and organizational measures to be taken by the (sub-) Processor to be able to provide assistance to the controller (and, for transfers from a Processor to a sub-Processor, to the data exporter).

Measure	Description
Self-service access to meet data subject rights of access, erasure, rectification etc.	Ability to login to review and edit Personal Data via the Cloudflare dashboard.