



**Crown
Commercial
Service**

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM155/ix) includes:

Part A - Order Form	2
Schedule 1 - Services	10
Schedule 2 - Call-Off Contract charges	8
Part B - Terms and conditions	8
Schedule 3 - Collaboration agreement	27
Schedule 4 - Alternative clauses	28
Schedule 5 - Guarantee	28
Schedule 6 - Glossary and interpretations	28
Schedule 7 - Processing, Personal Data and Data Subjects	
Schedule 7A - Data Processing Addendum	

Part A - Order Form

Digital Marketplace service ID number:	6253 7823 3095 524
Call-Off Contract reference:	CQC ICTC 627a
Call-Off Contract title:	Cornerstone Licences
Call-Off Contract description:	Licences and Service Agreement
Start date:	02/07/2018
Expiry date:	01/07/2020
Call-Off Contract value:	£130,000.00 (based on initial two year period)
Charging method:	Annual Fees are invoiced annually in advance, beginning on the Start Date, and then on each anniversary thereafter until the Expiry Date. Invoices shall be due within 30 days of the
Purchase order number:	To be provided following contract signature

This Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

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 Deliverables 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	Care Quality Commission 151 Buckingham Palace Road Victoria London SW1W 9SZ
To: the Supplier	Cornerstone OnDemand Ltd 4 Coleman Street, London EC2R 5AR Company number: 07143111
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: DIRECTOR OF PEOPLE Name: [REDACTED] Email: [REDACTED] Phone: [REDACTED]
For the Supplier:	Title: [REDACTED] Name: [REDACTED] Email: [REDACTED] Phone: [REDACTED]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 02/07/2018 and is valid for 24 months
--------------------	--

Ending (termination):	<p>The notice period needed for Ending the Call-Off Contract is at least fifteen [15] Working Days from the date that one party issues a notice to the other party stating details of a material breach (and such breach is then not cured).</p> <p>The Buyer may End the Call-Off Contract without cause at any time after the first anniversary of the Start Date, subject to giving at least 30 days' written notice to the Supplier.</p>
Extension period:	<p>This Call-Off Contract can be extended by the Buyer for up to 12 months, by giving the Supplier 3 month written notice before its expiry.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

Buyer contractual details

The Buyer hereby acknowledges and agrees to be bound by the Buyer that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2 – Cloud software (SaaS) G Cloud 9
G-Cloud services required:	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> Provision of Performance and Learning Clouds for 3,550 subscribers
Additional services:	N/A
Location:	<p>Software Hosted – UK</p> <p>Implementation Services – 151 Buckingham Palace Road, Victoria, London SW1W 9SZ</p>

Quality standards:	The quality standards required for this Call-Off Contract are as per the framework and G Cloud 9
Technical standards:	N/A
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are in the Supplier's Service Definition
On boarding:	The supplier will be expected to deploy the appropriate resource to facilitate delivery of the service. No implementation is required as Cornerstone already delivers the service to CQC.
Off boarding:	N/A
Collaboration agreement:	N/A
Limit on Parties' liability:	<p>The annual total liability of either Party for all Property defaults will not exceed the Charges payable by the Buyer to the Supplier hereunder for the twelve month period immediately preceding the date the cause of action arose.</p> <p>The annual total liability for Buyer Data defaults will not exceed the Charges payable by the Buyer to the Supplier hereunder for the twelve month period immediately preceding the date the cause of action arose.</p> <p>The annual total liability for all other defaults will not exceed the Charges payable by the Buyer to the Supplier hereunder for the twelve month period immediately preceding the date the cause of action arose.</p>
Insurance:	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> ● a minimum insurance period during the term of this Call-Off Contract] ● Professional indemnity insurance cover to be held by the Supplier s. This professional indemnity insurance cover will have a minimum limit of indemnity of [REDACTED] aggregate (and as required by Law)]

	<ul style="list-style-type: none"> ● employers' liability insurance with a minimum limit of [REDACTED] any higher minimum limit required by Law
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 90 consecutive days.
Audit:	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.</p> <p>The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the:</p> <ul style="list-style-type: none"> ● operation of the Framework Agreement and the Call-Off Contracts entered into with Buyers ● Services provided under any Call-Off Contracts (including any Subcontracts) ● amounts paid by each Buyer under the Call-Off Contracts <p>During the timeframes highlighted in clause 7.6, the Supplier will maintain:</p> <ul style="list-style-type: none"> ● commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations ● books of accounts for this Framework and all Call-Off Contracts ● MI reports ● access to its published accounts and trading entity information ● proof of its compliance with its obligations under the Data Protection Act and the Transparency provisions under this Framework Agreement ● records of its delivery performance under each Call-Off Contract, including that of its Subcontractors <p>The Supplier will allow the representatives of CCS, Buyers receiving Services, the auditors appointed by the Audit Commission access to the records, documents, and account information or, as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review:</p> <ul style="list-style-type: none"> ● the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement) ● any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only ● the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier ● any other aspect of the delivery of the Services including to review compliance with any legislation ● the accuracy and completeness of any MI delivered or required by the Framework Agreement ● any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records ● the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date

Buyer's responsibilities:	<p>The Buyer is responsible for:</p> <ul style="list-style-type: none"> • the Buyer is responsible for granting of access to the Buyers head office at 151 Buckingham Palace Road, London and any other premises for the delivery of the service • Active Users' compliance with the Agreement and liable for Active Users' breach thereof; • ensuring that it has obtained all necessary consents and approvals for Supplier to access Buyer Data for the purposes permitted under this Agreement; • Ensuring an adequate internet connection is in place to access the software; • Ensuring that only Buyer and its affiliates use the software for its own lawful business purposes; • Not using or deploying the software in violation of applicable laws; • Not reselling any software; • Not creating any derivative works based upon the software;
Buyer's equipment:	N/A

Supplier's information

Subcontractors or partners:	<p>Subprocessors are as follows:</p> <ul style="list-style-type: none"> • Cornerstone OnDemand Inc (USA) • Cornerstone OnDemand Spain S.L (Spain) • Cornerstone OnDemand Global Operations, Inc. (Israel) • Cornerstone OnDemand ANZ (New Zealand) • Cornerstone OnDemand Services India Private Limited (India) <p>The Data Processing Addendum at Schedule 7A details these subprocessors further.</p>
------------------------------------	---

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 by Bacs
Payment profile:	The payment profile for this Call-Off Contract is annually in advance.

Invoice details:	The Supplier will issue electronic invoices annually. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice
Who and where to send invoices to:	Invoices will be sent to the following address: Care Quality Commission T70 Payable F175 Phoenix House Topcliffe Lane Wakefield WF3 1WE. Email: CQCFinanceLiasonTeam@cqc.org.uk
Invoice information required	All invoices must include a valid purchase order number and sent to the above address or email address to enable payment.
Invoice frequency:	Invoice will be sent to Buyer annually in advance
Call-Off Contract value:	The total value of this Call-Off Contract is £130,000 (exclusive of any extension options and excluding VAT)
Call Off Contract charges:	Annual Fees are invoiced annually beginning on the Start Date through to the Expiry Date; £65,000 per annum

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following milestones:
Guarantee:	N/A
Warranties, representations:	N/A
Supplemental requirements in addition to the Call-Off terms:	N/A
Alternative clauses:	N/A
Buyer specific amendments	N/A

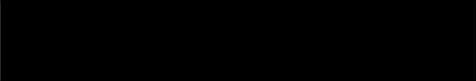
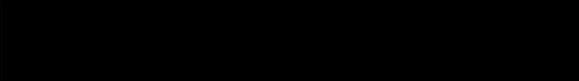
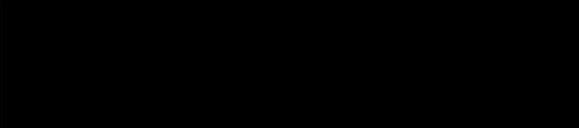
to/refinements of the Call-Off Contract terms:	
Public Services Network (PSN):	N/A
Personal Data and Data Subjects:	Will Schedule 7 – Processing, Personal Data and Data Subjects be used - Yes

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

2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557ix.
- (B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Cornerstone OnDemand Limited	Care Quality Commission
Name:		
Title:		
Signature:		

Date:		
--------------	--	--

Schedule 1 – Services

CSOD are providing software and associated services which are under Lot 2

The service shall comprise the Learning and Performance Clouds and associated sub modules e.g. Dashboards, together with associated integrated services.

The Software will be delivered as a SaaS model for the [redacted] active users identified. The software system will cover a Learning Management system with e-Learning, instructor led training, virtual classrooms, learning content management, with the performance cloud providing Competency assessments, development plans, goal setting, Performance reviews, and observation checklists.

Schedule 2 – Call-Off Contract charges

Supplier’s Digital Marketplace 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:

Product Name	Max Quantity of Subscribers	Annual Fee(s)
Performance	[REDACTED]	
Certifications		
Learning		
Competency Management		
Data Load Wizard		
Basic Training		
ANNUAL FEE SUBTOTAL		£65,000.00

Learning Cloud (Learning certificates, Competencies modules) per annum: £30,000.00 (based on there being a maximum of [REDACTED] subscribers)

Performance module per annum: £30,000 (based on there being a maximum of [REDACTED] subscribers)

[REDACTED]

SPECIAL TERMS

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 24 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, as long as this is within the maximum permitted under the

Framework Agreement of 2 periods of up to 12 months each.

- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 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:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)

- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)

- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'
- 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 Framework Agreement incorporated clauses will be referred to as incorporated Framework clause XX, where 'XX' is the Framework Agreement clause number.

2.4 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:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- 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 if the Supplier is delivering the Services Inside IR35.

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

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

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

5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - have raised all due diligence questions before signing the Call-Off Contract
 - have entered into the Call-Off Contract relying on its 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
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 7.9 for Buyer's failure to pay undisputed sums of money or if a dispute continues for more than three months. 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 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:

- 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

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

with this clause:

- a broker's verification of insurance
- receipts for the insurance premium
- 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:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances

- 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:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 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 the Data Protection Legislation or under incorporated Framework Agreement clauses 8.83 to 8.91. 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 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish

the IPR as open source.

- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown 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:
- rights granted to the Buyer under this Call-Off Contract
 - Supplier's performance of the Services
 - use by the Buyer of the Services
- 11.6 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:
- modify the relevant part of the Services without reducing its functionality or performance
 - 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
 - buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.7 Clause 11.5 will not apply if the IPR Claim is from:
- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
 - other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, 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:

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

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- 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

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

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

- 13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.3 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 policy and all Buyer requirements in the Order Form.
- 13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
- The principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
 - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach-sensitive-information-and-assets>
 - the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/guidance/risk-management-collection>
 - 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, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
 - the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at

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

- 13.6 The Buyer will specify any security requirements for this project in the Order Form.
- 13.7 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.
- 13.8 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.
- 13.9 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 available 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 software and the most up-to-date antivirus definitions available from an industry accepted antivirus software vendor 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:
- 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
 - 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 CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer 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, available at <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:
- an executed Guarantee in the form at Schedule 5
 - 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 the notice to the Supplier 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:
- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
 - Call-Off Contract Charges paid during the notice period is reasonable

compensation and covers 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:
- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
 - any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- 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
 - an Insolvency Event of the other Party happens
 - 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:
- any rights, remedies or obligations accrued before its Ending or expiration
 - the right of either Party to recover any amount outstanding at the time of Ending or expiry
 - the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses: 4 (Payment), 5 (Liability) and 6 (Litigation) (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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)
 - 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:
- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
 - return any materials created by the Supplier under this Call-Off Contract if the IPRs

are owned by the Buyer

- 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
- 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
- work with the Buyer on any ongoing work
- 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	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an 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 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 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
- 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 extend the Term beyond 24 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:
- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- 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:

- 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
- 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
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- 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:

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more

than the number of consecutive days set out in the Order Form, 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 4.2 to 4.7, each Party's total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or

statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

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:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- 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)

Section not applicable

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:

- the activities they perform

- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents

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:
- its failure to comply with the provisions of this clause
 - 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 does not 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 in the form set out in Schedule 3.

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

- work proactively and in good faith with each of the Buyer's contractors
- 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 The relationship between the Buyer and the Supplier is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).
- 33.2 The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment before commencing any processing (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.
- 33.3 The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take

into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

- i) are aware of and comply with the Supplier's obligations under this Clause;
- ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor
- iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract
- iv) are given training in the use, protection and handling of Personal Data.

unless the prior written consent of the Buyer has been obtained and

- i) the Buyer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer;
- ii) the Data Subject has enforceable rights and effective legal remedies;
- iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Buyer in meeting its obligations); and
- iv) the Supplier complies with any reasonable instructions notified to it in advance

by the Buyer with respect to the processing of the Personal Data.

- 33.6 The Supplier will delete or return (via the retrieval functionality of the Software) Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.
- 33.7 The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in accordance with any timescales reasonably required by the Buyer.
- 33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
- i) the Buyer determines that the processing is not occasional;
 - ii) the Buyer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal
 - iii) the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 33.9 Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.
- 33.10 The Buyer may amend this Call-Off Contract on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 4 - Alternative clauses

The Alternative clauses are available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 5 - Guarantee

The Guarantee is available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) 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 Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).

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 Representative	<p>purposes of, or in connection with, this Call-Off Contract.</p> <p>The representative appointed by the Buyer under this Call-Off Contract.</p>
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 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	Data, personal data and any information, which may include (but isn't limited to) any: <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
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 Data Protection Legislation.
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	Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach.
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Data Protection Legislation	<p>Data Protection Legislation means:</p> <ul style="list-style-type: none"> i) all applicable Law about the processing of personal data and privacy; and ii) The GDPR, the Regulation (EU) 2016/679, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and codes of practice issued by the Information Commissioner; and iii) to the extent that it relates to processing of personal data and privacy, any Laws that come into force which amend, supersede or replace existing Laws including the GDPR, the LED and any applicable national implementing Laws as amended from time to time including the DPA 2018 [subject to Royal Assent].
Data Subject	Takes the meaning given in the Data Protection Legislation.
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)

	<ul style="list-style-type: none"> ● 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>
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
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 outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	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: http://tools.hmrc.gov.uk/esi
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 <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 RM1557ix 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 Section 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.
GDPR	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.

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.
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	Can be: <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.
Intellectual Property Rights or IPR	Intellectual Property Rights are: <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

	<p>registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</p> <ul style="list-style-type: none"> ● 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 C61 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 CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.

LED	Law Enforcement Direction (Directive (EU) 2016/680).
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 provided to Dovers (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 section 6 (What you report to CCS).
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 Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	This has the meaning given in the Data Protection Act 1998 as amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	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: <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

	<ul style="list-style-type: none"> ● 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 pseudonymising and encrypting Personal Data ensuring confidentiality, integrity, availability and resilience of 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).
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 is not limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
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-controls-check-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.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
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 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 - Processing, Personal Data and Data Subjects

The parties acknowledge that for the purpose of the Data Protection Legislation, the Customer is the Controller and the Contractor is the processor.

Subject matter of the processing:

the subject matter of the processing will primarily consist of employee data

Duration of the processing:

From the Start Date until the Expiry Date (unless extended)

Nature and purposes of the processing:

Personal Data may be Processed for the following purposes:

- Delivery and use of human capital management software, including:
 - (a) For the Learning Suite, processing of the Buyer's employees' personal data shall be in order to monitor and manage the relevant employee's ongoing learning and development;
 - (b) For the Performance Suite, processing of the Buyer's employees' personal data shall be in order to monitor the relevant employee's ongoing performance and competencies.
- Implementation services related to configuration of human capital management software
- Product support
- Technical projects
- As further described in Cornerstone OnDemand's SSAE16 audit report, ISO27001 audit report, and IT security policy.

Type of Personal Data:

The Personal Data transferred may concern the following categories of data:

Learning, performance, recruiting and/or HR data

Categories of Data Subject:

The Personal Data transferred may concern the following categories of data subjects:

- Employees, suppliers, contractors, agents, directors, officers, members, and/or partners of the data controller and/or its affiliates

Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data:

Buyer may retrieve Buyer Personal Data any time prior to termination or expiration of the Call-Off Contract. If requested, Supplier will assist with such data retrieval at a scope and price to be agreed. Promptly upon the

expiration or earlier termination of the Call-Off Contract, Supplier shall securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Buyer Personal Data in Supplier's possession, custody or control. Notwithstanding the above, backups of Buyer Personal Data are to be deleted according to and in compliance with Supplier's general backup cycle, which means that backups will be deleted at the latest within approximately six (6) months from the decommissioning of Buyer's portal

Schedule 7A – Data Processing Addendum

DATA PROCESSING ADDENDUM

Preamble

This Data Processing Addendum (the "Addendum") forms part of and is subject to the terms of the master agreement executed by the Parties (the "Master Agreement") concerning the provisioning of human capital management software by the undersigned Cornerstone entity (hereinafter also "Cornerstone" or the "Processor") to Client (hereinafter also the "Controller"). It applies to all activities carried out by the Processor within the framework of the Master Agreement whereby the Processor's employees or third parties commissioned by the Processor might Process Personal Data of the Controller and/or its users.

1 Definitions

- 1.1 "Personal Data" means any information Processed by Cornerstone on behalf of Client relating to an identified or identifiable natural person, see article 4(1) of Regulation (EU) 2016/679 of 27 April 2016 (the "GDPR").
- 1.2 "Process" or "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see Article 4(2) of the GDPR).
- 1.3 "Third Country" means a country without a system of ensuring adequate protection within the meaning of Article 45 of the GDPR.
- 1.4 "Personal Data Breach" means, according to Article 4(12) of the GDPR, a 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.

Capitalized terms used, but not otherwise defined, herein shall have the same meanings assigned to those terms in the Master Agreement.

categories of data, the categories of data subjects and the purposes of the Processing set out in Annex 1.

3 Processing of Personal Data

- 3.1 Cornerstone shall Process Personal Data only in accordance with the Master Agreement and this Addendum, and in accordance with documented instructions listed in this Addendum and the Master Agreement, for the purposes of providing services under the Master Agreement. Client may issue further documented instructions consistent with and in the scope of this Addendum and the Master Agreement.
- 3.2 Cornerstone must notify Client in writing without undue delay regarding events which significantly impede Cornerstone's current or future ability to Process in accordance with this Addendum.
- 3.3 Cornerstone must limit the access to Personal Data to its employees or Subprocessors for whom access to said data is reasonably necessary to fulfill Cornerstone's obligations to Client. Cornerstone must ensure that persons authorized to Process the Personal Data are bound by the same or equivalent confidentiality obligations as Cornerstone and/or are under an appropriate statutory obligation of confidentiality.
- 3.4 Cornerstone shall implement and maintain appropriate technical and organizational measures as described in Article 32 of the GDPR. For this purpose, the Parties agree on the security measures set forth in Annex 2.

- 3.5 The appropriate technical and organizational security measures must be determined with due regard to:
- (i) the state of the art,
 - (ii) the cost of their implementation, and
 - (iii) the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 3.6 Cornerstone shall make available to Client upon request information necessary to demonstrate compliance with Processor's obligations set forth in Article 28 of the GDPR, and allow for and reasonably assist with audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, subject to the following:
- (i) The Controller mandates that Cornerstone shall at its own cost obtain and make available upon Client's request an audit report from an independent auditor regarding Cornerstone's compliance with the data security requirements of the controls defined in SSAE 16 SOC 2 or ISO 27001 (or equivalent standard). The audit report must be issued on the basis of a recognized standard for such audit reports.
 - (ii) In addition, Client is entitled, no more than once per year, at a time and scope to be agreed by the parties, and either directly or through an appointed independent auditor (other than a competitor of Cornerstone) to conduct an additional audit if and to the extent the audit set forth in the preceding paragraph does not meet the information requirements set forth in Article 28 of the GDPR. The auditor shall upon Cornerstone's request sign a customary non-disclosure agreement and treat all information obtained or received from Cornerstone confidentially, and may only share any information obtained with Client and Cornerstone. Client shall be responsible for costs of the audit, and agrees to pay Cornerstone a reasonable fee per audit to be mutually agreed by the parties to cover Cornerstone assistance with the audit. Notwithstanding the limitation of one audit per year, an additional audit may take place: (i) if required by a competent legal authority; or (ii) following a Personal Data Breach.
- 3.7 Cornerstone shall without undue delay notify Client about any:
- (i) request by a legal authority for disclosure of personal data processed under the agreement, unless the law requires otherwise;
 - (ii) request for access to Client Personal Data received directly from the data subjects themselves or from third parties.
- 3.8 Cornerstone shall notify Client without undue delay after becoming aware of a Personal Data Breach. The notification shall at least describe the nature of the Personal Data Breach (including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned) and the measures taken or proposed by Cornerstone to address the Personal Data Breach.
- 3.9 Cornerstone shall provide reasonable and timely assistance to Client (at Client's expense) to help enable Client to respond to: (i) any request from a data subject to exercise any of the data subject's rights under applicable data protection laws and regulations (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the Processing of the Personal Data.
- In the event that any such request, correspondence, enquiry or complaint is made directly to Cornerstone, Cornerstone shall promptly inform Client and provide full details of the same, except to the extent prohibited by law.
- 3.10 Cornerstone shall, upon Client's request and at Client's cost, reasonably assist the Controller in ensuring compliance with Controller's obligations pursuant to Articles 32 to 36 of the GDPR (including security of Processing,

notification of Personal Data breach, data protection impact assessment and prior consultation), based on the nature of Processing and the information available to Cornerstone.

4 Client's General Obligations

- 4.1 Client warrants that it will comply with all its obligations under applicable data protection laws and regulations.
- 4.2 Processing of any special categories of Personal Data (as defined in Article 9 of GDPR) may be subject to specific requirements and/or regulations depending on the relevant industry sector. In the event Client intends to Process any special categories of Personal Data, it will ensure that such Processing can be performed lawfully based on the current Services including the technical and organizational measures laid down in Schedule 2.

5 Other Data Processors

- 5.1 Cornerstone may engage other processors ("Subprocessors") for the Processing of Personal Data under this Addendum, provided Cornerstone ensures such Subprocessors' compliance with the terms of this Addendum. As of the effective date of the Addendum, Cornerstone currently relies on the Subprocessors listed in Annex 1 to provide the Services.
- 5.2 Prior to the engagement of another Subprocessor, Cornerstone shall inform Client of the intended subprocessing, thereby giving the Client the opportunity to object to such change on reasonable grounds, as set forth in Article 28 of the GDPR.
- 5.3 Client authorizes Cornerstone to transfer Client Data to Cornerstone Affiliates and/or other Subprocessors located in the United States, Israel, India, New Zealand and/or other locations outside the European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the Master Agreement, provided that, if Client is incorporated in the EU, either: (i) such locations are recognized by the European Commission as providing adequate data protection; (ii) Cornerstone has executed on behalf of Client (or its authorized proxy to Cornerstone), or (iii) upon Client's request, Client executes the EU standard contractual clauses directly with such Affiliates and/or other Subprocessors.
- 5.4 Cornerstone shall remain fully liable to the Client for the performance of its Subprocessors' obligations hereunder.
- #### 6 Data Retrieval and Deletion at Contract Termination
- 6.1 Client may retrieve its Personal Data prior to termination of the Master Agreement as set forth therein.
- 6.2 Promptly upon the expiration or earlier termination of the Master Agreement, Cornerstone shall securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Cornerstone's possession, custody or control.
- 6.3 Notwithstanding section 7.2, backups of Personal Data are to be deleted according to and in compliance with Cornerstone's general backup cycle, which means that backups will be deleted at the latest within approximately six (6) months from the decommissioning of Client's portal.
- 6.4 Cornerstone shall provide to Client, upon Client's request, written confirmation that deletion has occurred in accordance with this section 7.
- 6.5 In the event applicable law does not permit Cornerstone to comply with delivery or destruction of Personal Data

as set forth herein, Cornerstone shall ensure the privacy, confidentiality and security of the Personal Data in accordance with the standards agreed in this Addendum and shall not use or disclose any Personal Data after termination of the Master Agreement.

7 Miscellaneous

The Parties may agree in good faith on any reasonable amendment to the Addendum required to maintain compliance with the applicable law. Such amendment may include additional costs to be reasonably agreed by the parties.

The image shows a large, faint, and mostly illegible table or diagram, possibly a contract schedule or flowchart, located in the lower middle section of the page. The content is too light to transcribe accurately.

ANNEX 1**I. Categories of data, categories of data subjects and purposes of the Processing****a) Purpose and nature of the Processing operations**

Personal Data may be Processed for the following purposes:

- Delivery and use of human capital management software
- Implementation services related to configuration of human capital management software
- Product support
- Technical projects
- As further described in Cornerstone OnDemand's SSAE16 audit report, ISO27001 audit report, and IT security policy.

b) Categories of data subjects

The Personal Data transferred may concern the following categories of data subjects:

- Employees, suppliers, contractors, agents, directors, officers, customers, members, and/or partners of the data controller and/or its affiliates

c) Categories of Personal Data

The Personal Data transferred may concern the following categories of data:

- Learning, performance, recruiting, and/or HR data

d) Special categories of data**II. Current Subprocessors**

Subprocessor	Country	Services performed
Cornerstone OnDemand Inc.	U.S.A.	Support, R&D, Technical Project Services
Cornerstone OnDemand Spain S.L.	Spain	Support
Cornerstone OnDemand Global Operations, Inc.	Israel	Support
Cornerstone OnDemand ANZ	New Zealand	Support
Cornerstone OnDemand Services India Private Limited	India	Support, Technical Project Services

ANNEX 2

Security measures

(1) Cornerstone shall Process Personal Data in accordance with applicable law to which Cornerstone is subject and in accordance the data security requirements of the controls defined in SSAE 16 SOC 2 or ISO 27001 (or equivalent standard).

(2) Cornerstone shall appoint a fixed contact point for Client to carry out any matters in relation to the Processing of Personal Data.

(3) Cornerstone shall ensure that Cornerstone's employees receive adequate training and instructions, including, but not limited to, education on general safety awareness, relevant security policies and procedures, and Personal Data Processing.

(4) Cornerstone shall maintain organizational and technical measures to ensure separation of data between clients and systems.

(5) Access Control of Processing Areas

Cornerstone shall maintain suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data is Processed or used. This is accomplished by measures like:

- establishing security areas;
- protection and restriction of access paths;
- securing the decentralized telephones, data Processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations on card-keys;
- restriction on card-keys;
- all access to the data centre where Personal Data is hosted is logged, monitored, and tracked;
- the data centre where Personal Data is hosted is secured by a security alarm system; and
- other appropriate security measures.

(6) Access Control to Data Processing Systems

Cornerstone shall maintain suitable measures to prevent its Personal Data Processing systems from being used by unauthorized persons. This is accomplished by measures like:

- identification of the terminal and/or the terminal user to the Cornerstone systems;
- automatic time-out of user terminal if left idle, with identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered;
- log file of events (monitoring of break-in-attempts),
- issuing and safeguarding of identification codes;
- dedication of individual terminals and/or terminal users, and identification characteristics exclusive to specific functions;
- employee policies and training with respect to each employee's access rights to Personal Data (if any), including informing employees about their obligations and the consequences of any violations of such obligations, to ensure that employees will only access Personal Data and resources required to perform their job duties; and
- all access to data content is logged, monitored, and tracked.

(7) Access Control to Use Specific Areas of Data Processing Systems

Cornerstone commits that the persons entitled to use its Personal Data Processing system are only able to access the data within the scope and to the extent covered by its access permission (role or authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- employee policies and training with respect to each employee's access rights to the Personal Data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of Personal Data only to authorized persons;
- control of files, controlled and documented destruction of Personal Data; and
- policies controlling the retention of back-up copies.

(8) Availability Control

Cornerstone shall maintain suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy;
- tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for database server;
- complying with Cornerstone's business continuity policy; and
- any detected security incident is recorded

For all applications supported by the Cornerstone, the following controls will be implemented:

(9) Transmission Control

Cornerstone shall maintain suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of state of the art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within system transmission;
- as far as possible, all data transmissions are logged, monitored and tracked; and
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Cornerstone implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into Personal Data Processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and disposal of stored Personal Data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and disposal of stored Personal Data;
- utilization of user codes (passwords);
- following a policy according to which all employees of Cornerstone who have access to Personal Data Processed for Client shall reset their passwords at a minimum once in a 180 day period;
- providing that entries to Data Processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user IDs that have not been used for a substantial period of time;
- proof established within Cornerstone's organization of the input authorization; and
- electronic recording of entries.

(11) Cornerstone system administrators (if any):

Cornerstone shall maintain measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;

- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by importer and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Client upon request.

(12) Separation of Processing for different Purposes

Cornerstone shall maintain suitable measures to ensure that Personal Data collected for different purposes can be Processed separately. This is accomplished by:

- access to Personal Data is separated through application security for the appropriate users; and
- modules within Cornerstone's database separate which data is used for which purpose, i.e., by functionality and function.

Client acknowledges and agrees that Cornerstone may change its security policies and related security measures, provided that Cornerstone maintains, at all times, an overall level of security as least as stringent as the one set forth in this Addendum.

