



## G-Cloud 13 Call-Off Contract

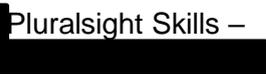
This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

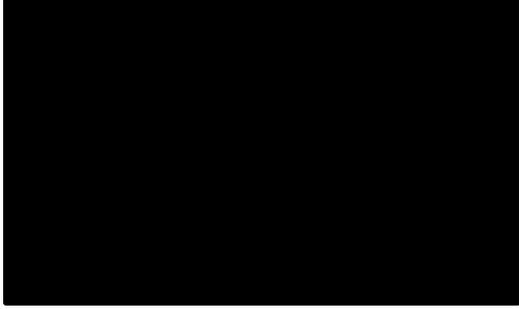
### **G-Cloud 13 Call-Off Contract**

Part A: Order Form	2
Part B: Terms and conditions	16
Schedule 1: Services	36
Schedule 2: Call-Off Contract charges	37
Schedule 3: Collaboration agreement	38
Schedule 4: Alternative clauses	39
Schedule 5: Guarantee	40
Schedule 6: Glossary and interpretations	41
Schedule 7: UK GDPR Information	61
Annex 1: Processing Personal Data	61
Annex 2: Standard Contractual Clauses	66

## Part A: Order Form

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

<b>Platform service ID number</b>	706676638210170
<b>Call-Off Contract reference</b>	DDaT24274
<b>Call-Off Contract title</b>	Technology training platform
<b>Call-Off Contract description</b>	Technology training platform
<b>Start date</b>	<b>7<sup>th</sup> September 2024</b>
<b>Expiry date</b>	<b>6<sup>th</sup> September 2026</b>
<b>Call-Off Contract value</b>	<p>The maximum Call-Off Contract value for the initial 24-month period shall not exceed \$24,950.00 excluding VAT.</p> <p>There is an optional 12-month extension period. The value for the optional extension period shall not exceed \$12,475.00 excluding VAT.</p> <p>(2-Year term):  Pluralsight Skills –                       totalling \$24,950.00 excluding VAT</p> 

	
<b>Charging method</b>	BACS
<b>Purchase order number</b>	TBC

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

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

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

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

<b>From the Buyer</b>	UK Research and Innovation Polaris House, North Star Avenue, Swindon SN2 1FL United Kingdom
-----------------------	---

<b>To the Supplier</b>	Pluralsight LLC 42 E Future Way Draper 840209858 Utah USA
<b>Together the 'Parties'</b>	

Principal contact details

**For the Buyer:**

Title: [REDACTED]  
Name: [REDACTED]  
Email: [REDACTED]  
Phone: [REDACTED]

**For the Supplier:**

Title: [REDACTED]  
Name: [REDACTED]  
Email: [REDACTED]  
Phone: [REDACTED]

Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on <b>7<sup>th</sup> September 2024</b> and is valid for <b>24 months</b> .
-------------------	---

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

### Buyer contractual details

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

<p><b>G-Cloud Lot</b></p>	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> <li>• Lot 2: Cloud software</li> </ul>
<p><b>G-Cloud Services required</b></p>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> <li>• Pluralsight Skills - Business Enterprise - [REDACTED]</li> </ul>
<p><b>Additional Services</b></p>	<p>Not applicable.</p>

<b>Location</b>	The Services will be delivered remotely to Polaris House, North Star Avenue, Swindon, SN2 1FL.
<b>Quality Standards</b>	The quality standards required for this Call-Off Contract are as detailed in the Supplier's Service Definition available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a>
<b>Technical Standards:</b>	The technical standards required for this Call-Off Contract are as detailed in the Supplier's Service Definition available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a>
<b>Service level agreement:</b>	The service level and availability criteria required for this Call-Off Contract are detailed in the Supplier's Service Definition available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a>
<b>Onboarding</b>	The onboarding plan for this Call-Off Contract is in the Supplier's Service Definition available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a>

<b>Offboarding</b>	The offboarding plan for this Call-Off Contract is in the Supplier's Service Definition available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a>
<b>Collaboration agreement</b>	Not applicable.

<p><b>Limit on Parties' liability</b></p>	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed <b>\$24,950.00</b> per year.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed <b>\$24,950.00</b> or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of <b>\$24,950.00</b> or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<p><b>Insurance</b></p>	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>● a minimum insurance period of [2 years] following the expiration or Ending of this Call-Off Contract</li> <li>● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)</li> <li>● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law</li> </ul>

<p><b>Buyer’s responsibilities</b></p>	<p>The Buyer is responsible for the process / systems required to obtain, create, manage and communicate information with relevant internal and external parties.</p> <p>The Buyer is responsible for activities as detailed within the Digital Marketplace published, Pluralsight Terms and Conditions available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a></p>
<p><b>Buyer’s equipment</b></p>	<p>N/A to SaaS</p>

Supplier’s information

<p><b>Subcontractors or partners – N/A</b></p> <p><b>Sub-processors</b></p>	<p>The Supplier’s list of Sub-processors is available at Supplier’s website <a href="https://www.pluralsight.com/terms/sub-processors">https://www.pluralsight.com/terms/sub-processors</a>.</p>
---	--

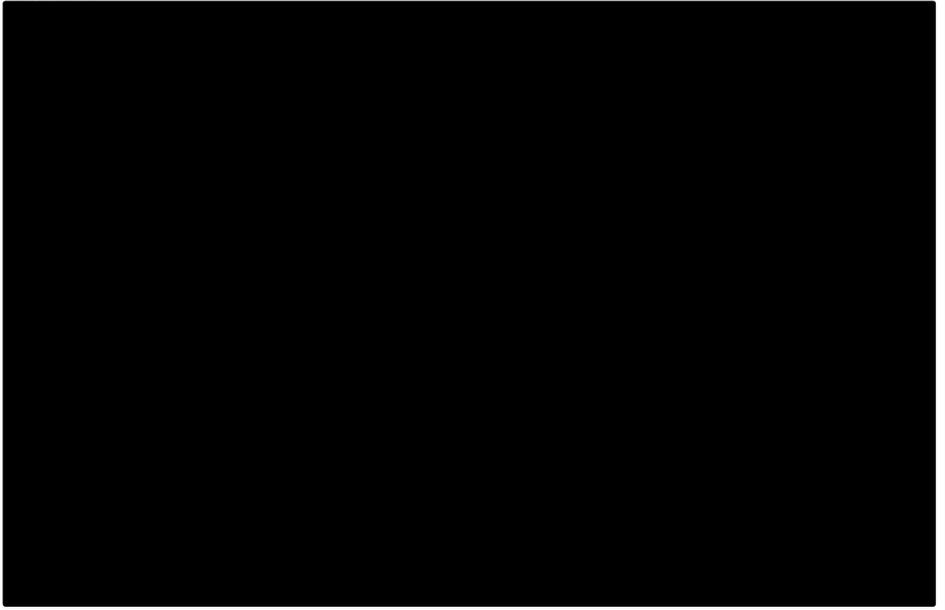
Call-Off Contract charges and payment

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

<p><b>Payment method</b></p>	<p>The payment method for this Call-Off Contract is BACS and upon receipt of a valid invoice.</p>
------------------------------	---

<b>Payment profile</b>	The payment profile for this Call-Off Contract is annually in advance.
<b>Invoice details</b>	The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
<b>Who and where to send invoices to</b>	Invoices will be sent to [REDACTED] and [REDACTED]
<b>Invoice information required</b>	All invoices must include a valid purchase order reference: <b>DDaT24274</b> .
<b>Invoice frequency</b>	Invoice will be sent to the Buyer annually in advance.

<b>Call-Off Contract value</b>	The total value of this Contract is \$24,950.00 excluding VAT.
--------------------------------	--

<b>Call-Off Contract charges</b>	The breakdown of the Charges is: Year 1 
----------------------------------	---

Additional Buyer terms

<b>Performance of the Service</b>	Not applicable.
-----------------------------------	-----------------

<b>Guarantee</b>	Not applicable.
<b>Warranties, representations</b>	No additional warranties or representation required.
<b>Supplemental requirements in addition to the Call-Off terms</b>	Within the scope of the Call-Off Contract, the Supplier requires the Buyer to enter into a data transfer agreement in the form of the European Commission's Standard Contractual Clauses (Controller to Processor) Module II and the Information Commission Office's (ICO) International Data Transfer Addendum to the EU Commission's Standard Contractual Clauses (SCC) with it as set out in Schedule 7, Addendum I
<b>Alternative clauses</b>	Not applicable.

<p><b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b></p>	<p>Not applicable.</p>
<p><b>Personal Data and Data Subjects</b></p>	<p>Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used:] <b>Annex 1</b></p>
<p><b>Intellectual Property</b></p>	<p>Other than the limited right to access Supplier’s platform during the term of this Call-Off Contract, no Intellectual Property rights of Supplier or any other party are granted to Buyer</p>
<p><b>Social Value</b></p>	<p>Please refer to our Social Value Statement in our Service Description available at <a href="https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170">https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/706676638210170</a></p>

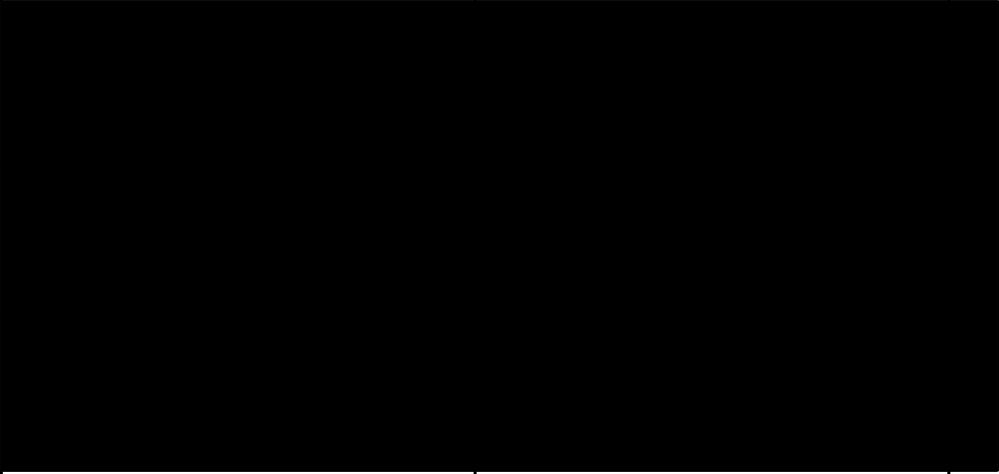
**1. Formation of contract**

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and

Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

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

<b>Signed</b>	Supplier	Buyer
<b>Name</b>		
<b>Title</b>		
<b>Signature</b>		
<b>Date</b>	3 October 2024	8 October 2024

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

## Customer Benefits

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

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

## Part B: Terms and conditions

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

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

### 2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
  - 2.3 (Warranties and representations)
  - 4.1 to 4.6 (Liability)
  - 4.10 to 4.11 (IR35)
  - 10 (Force majeure)
  - 5.3 (Continuing rights)
  - 5.4 to 5.6 (Change of control)
  - 5.7 (Fraud)
  - 5.8 (Notice of fraud)
  - 7 (Transparency and Audit)
  - 8.3 (Order of precedence)
  - 11 (Relationship)
  - 14 (Entire agreement)
  - 15 (Law and jurisdiction)
  - 16 (Legislative change)
  - 17 (Bribery and corruption)
  - 18 (Freedom of Information Act)
  - 19 (Promoting tax compliance)
  - 20 (Official Secrets Act)
  - 21 (Transfer and subcontracting)
  - 23 (Complaints handling and resolution)
  - 24 (Conflicts of interest and ethical walls)
  - 25 (Publicity and branding)
  - 26 (Equality and diversity)
  - 28 (Data protection)
  - 31 (Severability)

- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

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

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

### 4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

- 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
  - 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
  - 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
  - 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
  - 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
  - 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
  - 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
  - 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
  - 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.
5. Due diligence
- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
    - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
    - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
    - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
    - 5.1.4 have entered into the Call-Off Contract relying on their own due diligence
6. Business continuity and disaster recovery
- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

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

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoices under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

## 9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

- 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
- 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
- 9.8.1 premiums, which it will pay promptly
- 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer
10. Confidentiality
- 10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.
11. Intellectual Property Rights
- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance

with this Contract, including the right to grant sub-licences to Subcontractors provided that:

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

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

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

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

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

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

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

- 11.7.1 modify the relevant part of the Services without reducing its functionality or performance
  - 11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - 11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.8 Clause 11.6 will not apply if the IPR Claim is from:
- 11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.8.2 other material provided by the Buyer necessary for the Services
- 11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12. Protection of information

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

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

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

### 13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework:

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

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.npsa.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.npsa.gov.uk/sensitive-information-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

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

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

- 13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:  
<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
- 13.6.6 Buyer requirements in respect of AI ethical standards.
- 13.7 The Buyer will specify any security requirements for this project in the Order Form.
- 13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.
14. Standards and quality
- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:  
<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.
15. Open source
- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

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

## 16. Security

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

## 17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

## 18. Ending the Call-Off Contract

the

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

- 18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.
19. Consequences of suspension, ending and expiry
- 19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.
- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- 19.4.1 any rights, remedies or obligations accrued before its Ending or expiration
- 19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry
- 19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
- 7 (Payment, VAT and Call-Off Contract charges)
  - 8 (Recovery of sums due and right of set-off)
  - 9 (Insurance)
  - 10 (Confidentiality)
  - 11 (Intellectual property rights)
  - 12 (Protection of information)
  - 13 (Buyer data)
  - 19 (Consequences of suspension, ending and expiry)
  - 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)
- 19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

- 19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:
- 19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
  - 19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
  - 19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
  - 19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
  - 19.5.5 work with the Buyer on any ongoing work
  - 19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
- 19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
- 19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

## 20. Notices

- 20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.
- Manner of delivery: email
  - Deemed time of delivery: 9am on the first Working Day after sending
  - Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message
- 20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

## 21. Exit plan

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

- 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- 21.8.4 the testing and assurance strategy for exported Buyer Data
- 21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations
- 21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

## 22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

## 23. Force majeure

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

## 24. Liability

- 24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).
- 24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:
- 24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and
- 24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.
- 24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).
- 24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

## 25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.
- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
- 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
- 25.5.2 comply with Buyer requirements for the conduct of personnel
- 25.5.3 comply with any health and safety measures implemented by the Buyer

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

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

## 26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

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

## 28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

## 29. The Employment Regulations (TUPE)

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

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

to

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

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29. 2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

- 29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.5 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
  - 29.5.1 its failure to comply with the provisions of this clause
  - 29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

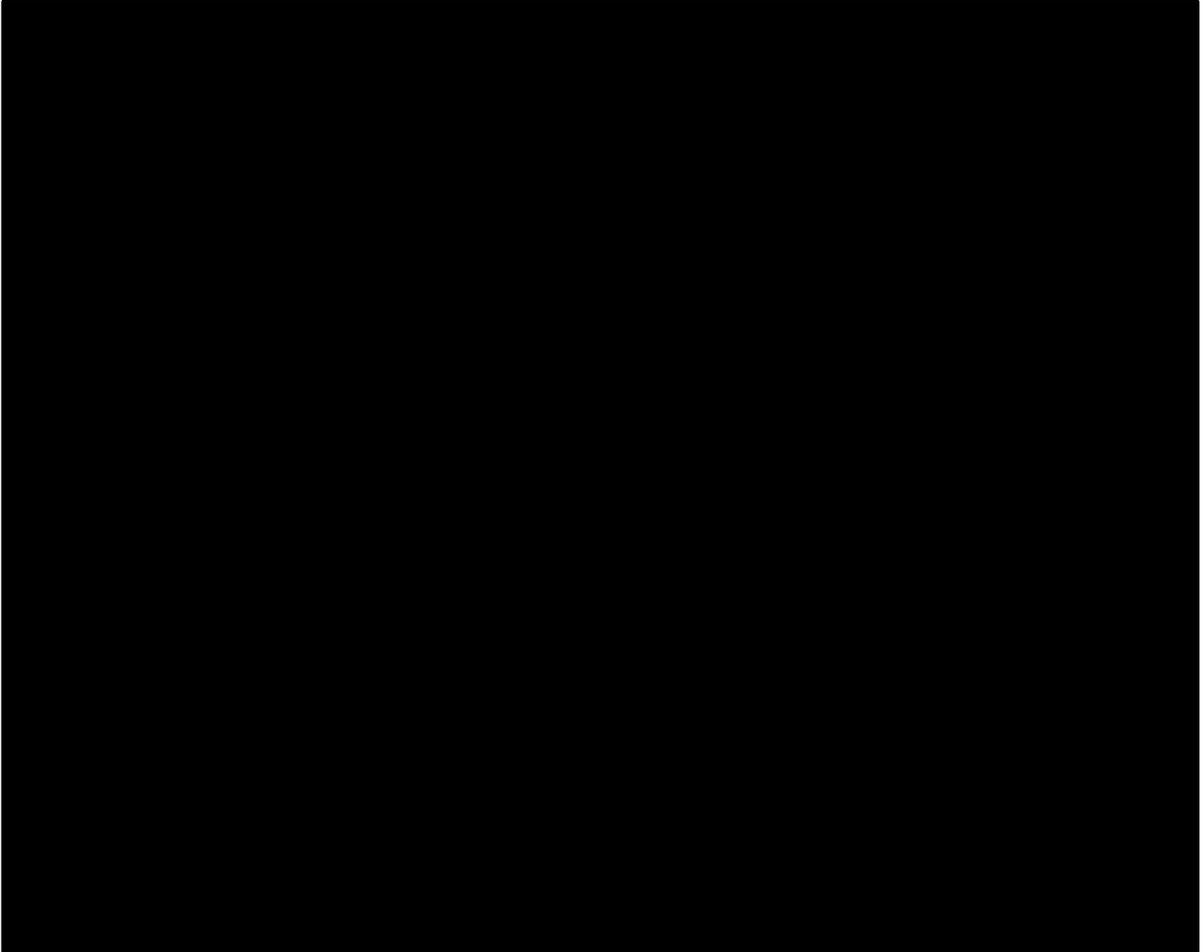
- 29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.
30. Additional G-Cloud services
- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.
31. Collaboration
- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
- 31.2.1 work proactively and in good faith with each of the Buyer's contractors
- 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services
32. Variation process
- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.
33. Data Protection Legislation (GDPR)
- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

## Schedule 1: Services



## Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:



## Schedule 3: Collaboration agreement

Not applicable.

## Schedule 4: Alternative clauses

Not applicable.

## Schedule 5: Guarantee

Not applicable.

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

<b>Expression</b>	<b>Meaning</b>
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses.
<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>• owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>• created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>

<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.
<b>Buyer Software</b>	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
<b>Call-Off Contract</b>	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
<b>Confidential Information</b>	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> <li>• information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

<b>Controller</b>	Takes the meaning given in the UK GDPR.
<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b>	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
<b>Data Protection Legislation (DPL)</b>	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
<b>Data Subject</b>	Takes the meaning given in the UK GDPR

<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

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

<p><b>Force Majeure</b></p>	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<p><b>Former Supplier</b></p>	<p>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).</p>
<p><b>Framework Agreement</b></p>	<p>The clauses of framework agreement RM1557.13 together with the Framework Schedules.</p>

<b>Fraud</b>	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.
<b>Freedom of Information Act or FoIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
<b>UK GDPR</b>	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.

<p><b>Inside IR35</b></p>	<p>Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.</p>
<p><b>Insolvency event</b></p>	<p>Can be:</p> <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> <li>• a Dun &amp; Bradstreet rating of 10 or less</li> </ul>
<p><b>Intellectual Property Rights or IPR</b></p>	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> <li>• copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</li> <li>• applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>
<p><b>Intermediary</b></p>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
<b>Law</b>	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.

<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement Schedule 6.
<b>Material Breach</b>	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

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

<b>Personal Data</b>	Takes the meaning given in the UK GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the UK GDPR.
<b>Platform</b>	The government marketplace where Services are available for Buyers to buy.
<b>Processing</b>	Takes the meaning given in the UK GDPR.
<b>Processor</b>	Takes the meaning given in the UK GDPR.

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

<p><b>Project Specific IPRs</b></p>	<p>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.</p>
<p><b>Property</b></p>	<p>Assets and property including technical infrastructure, IPRs and equipment.</p>
<p><b>Protective Measures</b></p>	<p>Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.</p>

<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.

<b>Replacement supplier</b>	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Platform.

<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.

<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
<b>Supplier Terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.

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

## Schedule 7: UK GDPR Information

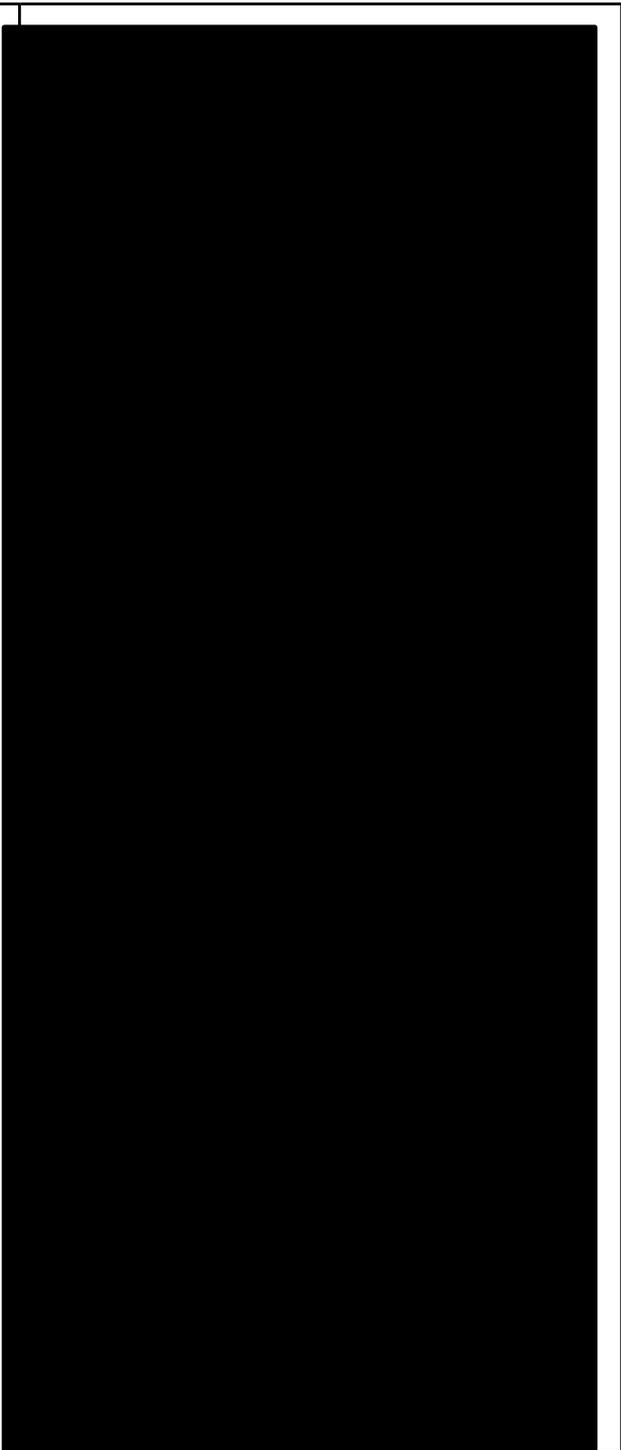
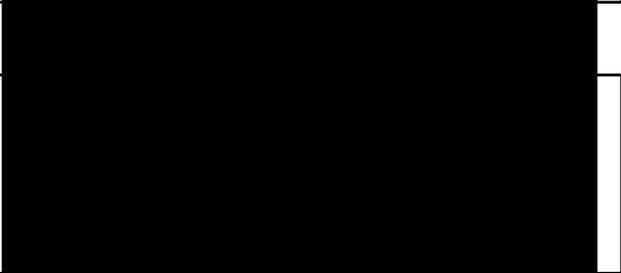
This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

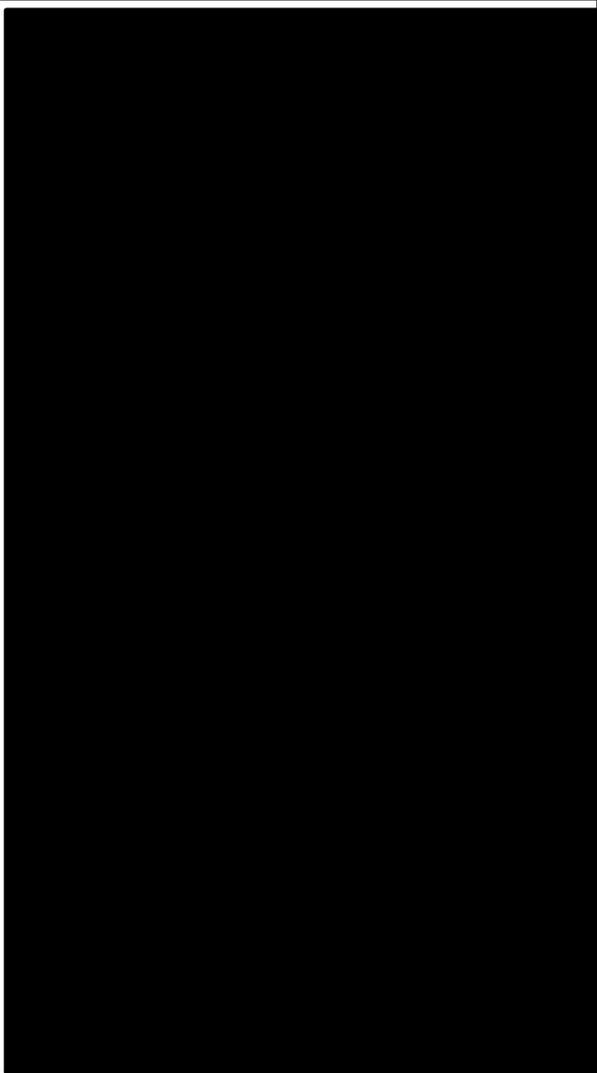
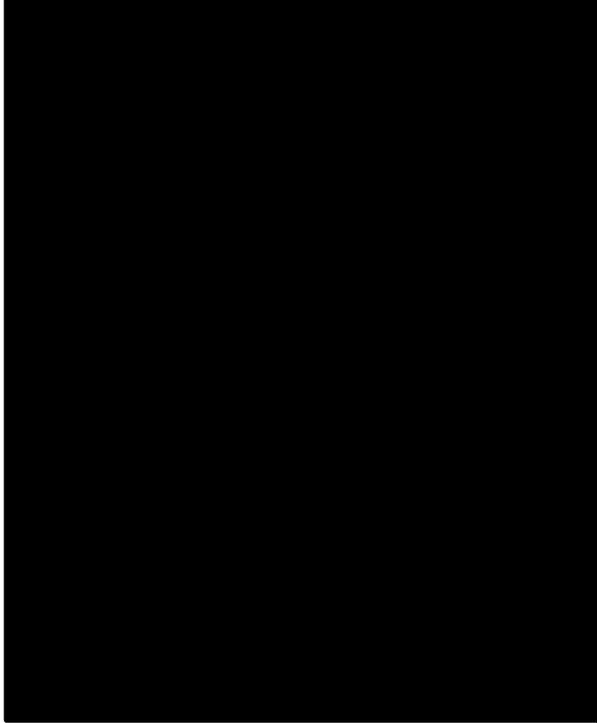
### Annex 1: Processing Personal Data

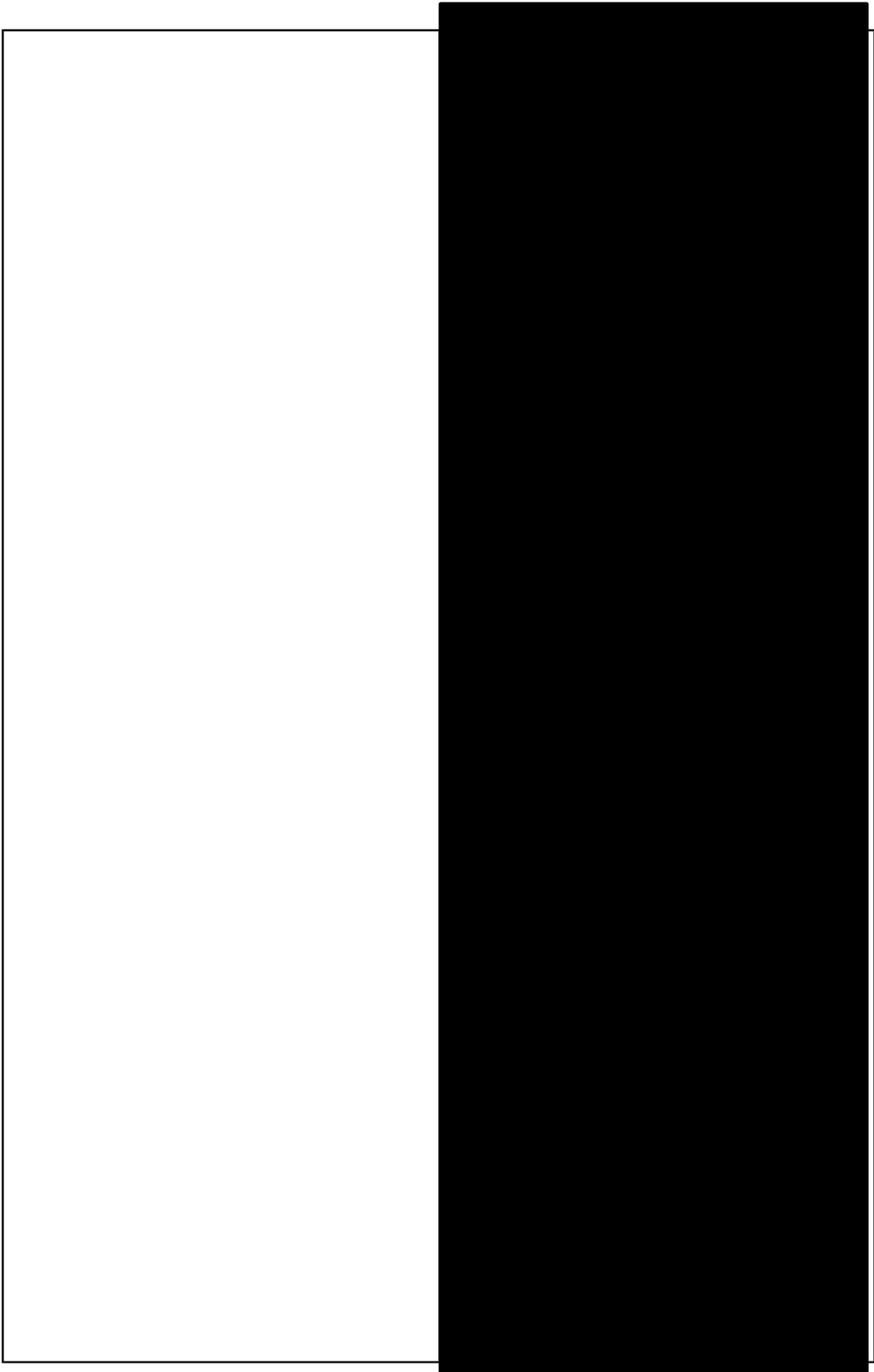
This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

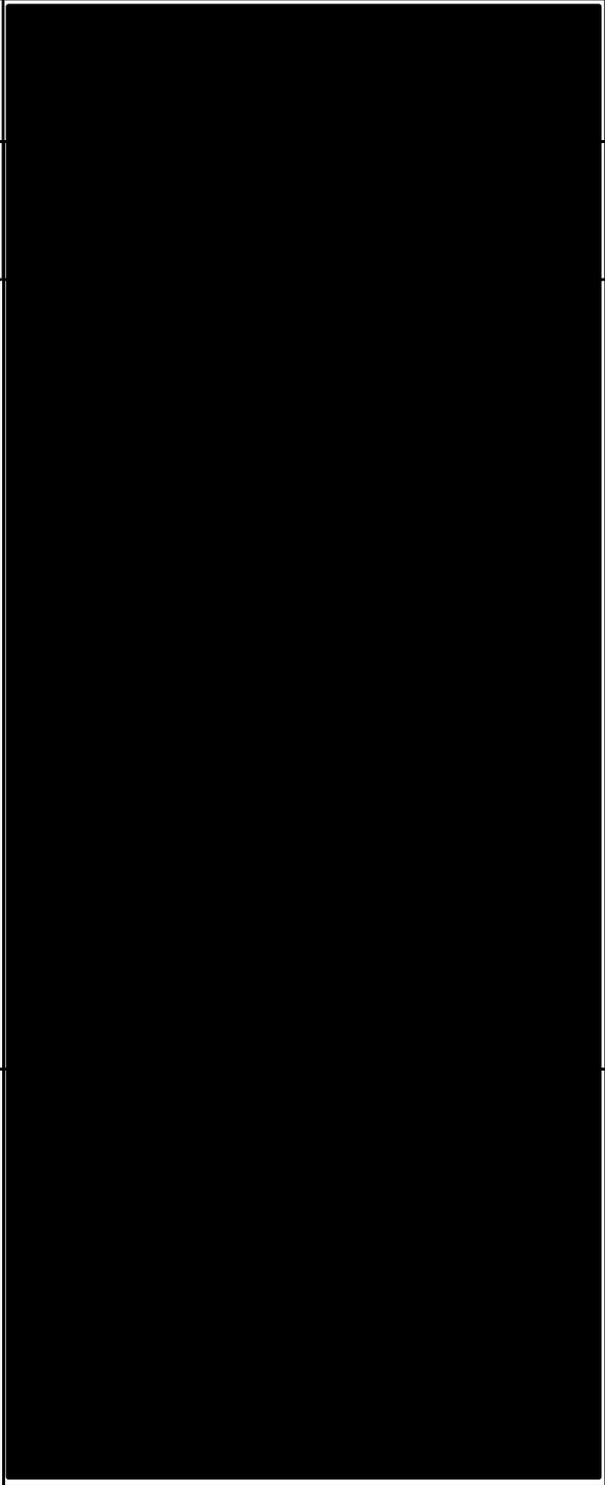
- 1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: : Pluralsight Privacy Team [REDACTED] ; with a copy to: [REDACTED] )
- 1.3 The Processor shall comply with any further written instructions with respect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

Description	Details
Identity of Controller for each Category of Personal Data	[REDACTED]

<p>Duration of the Processing</p>	
	

<p>Nature and purposes of the Processing</p>	
<p>Type of Personal Data</p>	



		
Categories of Data Subject		
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data		

## Annex 2 – Standard Contractual Clauses (Controller to Processor) Module II

### SECTION I

#### *Clause 1*

##### **Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) <sup>1</sup> for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)
- have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### *Clause 2*

##### **Effect and invariability of the Clauses**

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

---

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ([OJ L 295, 21.11.2018, p. 39](#)), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/91.

### **Clause 3**

#### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18(a) and (b)
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **Clause 4**

#### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **Clause 5**

#### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **Clause 6**

#### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### **Clause 7 – Intentionally Left Blank**

## SECTION II – OBLIGATIONS OF THE PARTIES

### *Clause 8*

#### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under

Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union <sup>2</sup>(in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## 8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### **Clause 9**

#### **Use of sub-processors**

- (a) **GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

<sup>2</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. <sup>3</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10**

##### **Data subject rights**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11**

##### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

---

<sup>3</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## **Clause 12**

### **Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

## **Clause 13**

### **Supervision**

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in

which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

#### *Clause 14*

##### **Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>4</sup>;

<sup>4</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### **Clause 15**

#### **Obligations of the data importer in case of access by public authorities**

##### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it.
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on

the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## 15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

#### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17**

##### **Governing law**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of **The Republic of Ireland** (*specify Member State*).]

#### **Clause 18**

##### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of The Republic of Ireland (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

#### **APPENDIX**

##### **EXPLANATORY NOTE:**

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

**Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...



Role (controller/processor): ...Controller  
...

**Data importer(s):** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...Pluralsight, LLC

Address: ...42 Future Way, Draper, UT 84020

Contact person's name, position and contact details:



Associate General Counsel,  
Contracts

Activities relevant to the data transferred under these Clauses: ...For the provision of SaaS Products.

Signature and date: ... 3 October 2024



Role (controller/processor): ...Processor

## B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

... **Data subjects:** *Data subjects include the Customer's representatives and end-users including employees, contractors, and collaborators. Pluralsight acknowledges that, depending on Customer's use of the Products, Customer may elect to include personal data from any of the following types of data subjects in the personal data:*

- *Employees, contractors and temporary workers (current, former, prospective) of data exporter; and*
- *Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former).*

*Categories of personal data transferred*

... **Categories of data:** *The personal data that is uploaded to the Platform and included in email, documents and other data in an electronic form in the context of the Products. Pluralsight acknowledges that, depending on Customer's use of the Products, Customer may elect to include personal data from any of the following categories in the personal data:*

- *Basic personal data (for example street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, screen name/handle, email address);*
- *Authentication data (for example user name/handle, password, security question, audit trail);*
- *Contact information (for example physical addresses, email, phone numbers, social media identifiers);*
- *Unique identification numbers such as IP addresses, employee number, student number, unique identifier in tracking cookies or similar technology);*
- *Pseudonymous identifiers;*
- *Commercial Information (for example history of purchases, special offers, subscription information, payment history);*
- *Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);*
- *Photos, video and audio;*
- *Internet activity (for example browsing and search history while on the Platform);*
- *Device identification (for example IMEI-number, SIM card number, MAC address);*
- *Profiling (for example based on pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);*
- *Employment data derived from a data subject's association with a commercial customer (for example job and position data);*
- *Education data (for example degree and certification history);*
- *Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or*
- *Any other personal data identified in Article 4 of the GDPR.*

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

... *Not applicable*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*... On a continuous basis as necessary for the data importer to meet its obligations in conjunction with the provision of the SaaS services for the term of the agreements with the data exporter.*

*Nature of the processing*

*...The nature and purpose of the processing shall include the collection, organisation, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the personal data as necessary to provide the products or services pursuant to the agreements with data exporter.*

*Purpose(s) of the data transfer and further processing*

*...Personal data will be processed in conjunction with data exporter's Agreements to allow the data importer to fulfill its obligations thereunder.*

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*...Personal data will be retained for so long as the user(s) continue to maintain and use their accounts. Dormant accounts are checked intermittently and where contact cannot be made with the user to confirm their intent to maintain the account, the account is canceled. Upon such cancelation all data associated with that account will no longer be identifiable to a natural person.*

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*...Sub-processors are retained in support of the SaaS products/services provided to data exporters and are contractually bound as to subject matter, nature and duration of the processing similarly in kind as the data importer taking into account the sub-processors specific role.*

### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identification of the competent supervisory authority/ies in accordance with Clause 13*

***If the data exporter is established in an EU Member State:*** the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.

***If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR):*** the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.

***If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU:*** the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.

## ANNEX II

( Platform - <https://www.pluralsight.com> )

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*
- *The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.*
- *Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.*
- *The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.*
- *All corporate endpoint devices/laptops are encrypted using NIST standard encryption algorithms at the disk or volume level leveraging technologies incorporated in the operating system.*
- *Application credentials and service accounts are encrypted and stored in centrally managed solutions.*
- *Amazon RDS Databases are encrypted at the database level using NIST AES standard of 128 bit encryption or higher.*
- *Pluralsight does not ever store credit card information in our data stores; rather, Pluralsight utilizes third-party services, which are PCI-certified and implement industry data security standards appropriate for that data classification, to manage all confidential subscription and billing information.*
- *The Pluralsight platform leverages the bcrypt hashing algorithm for all individual customer passwords and only ever stores the hashed output of that computation.*

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

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

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

- *Pluralsight's production environment is housed in the AWS US-West-2 Region. High Availability (HA) is turned on for critical services. The AWS infrastructure provides redundancy for Pluralsight platform availability.*
- *The App.Pluralsight.com Disaster Recovery Plan is activated when an event is determined to significantly affect or threaten to significantly affect The Pluralsight Skills product. The degree and extent of activation depends upon the impact and timing of the event, but for the purposes of this plan, a disaster will be declared when the primary Amazon region hosting app.pluralsight.com is unavailable and the*

## OFFICIAL

*Estimated Time to Resolution(ETR) for that region is less than our projected ETR for recovering to a different Amazon region. Specific actions to be undertaken upon disaster declaration and plan activation are detailed hereafter. Both our RTO and RPO are 24 hrs. Those objectives are what we will compare with AWS's ETR.*

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

- *Disaster Recovery Testing is conducted quarterly*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Measures for user identification and authorization.*
- *Centralized directory (Okta) integration with ticketing system and HRIS systems auto provisions access for the team member with appropriate access for their role.*
- *Any additional requests for access to IT systems not managed by the IT team are requested by the team member and/or manager to the application owner.*
- *Team members shall be positively identified, authorized, and authenticated before they are granted access to company information resources.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Access to information resources shall be controlled through a defined and managed process which addresses authorizing, modifying, and revoking access, and which includes a periodic review of information system privileges.*
- *A user enrollment process shall be created, documented, implemented, and maintained on a regular basis.*
- *Each user shall be uniquely identified.*
- *Each user requiring access to Pluralsight's information assets above the standard access for their job function shall submit a request*
- *User access requests shall be retained as required by business and regulatory needs.*
- *Information resources and network services shall not be accessible to users unless the user has been explicitly authorized and granted permission to access the resource or service.*
- *The allocation and use of privileges shall be restricted and managed.*
- *User privileges shall be tracked at the application level and each user's profile (identity, access, privileges, and authorization) recorded and managed to prevent misuse of resources.*
- *Authentication tokens (i.e., passwords) and keys for privileged users must be rotated upon termination.*
- *User access and privileges shall be reviewed through a defined process.*
- *Reviews of non-administrative and administrative user access rights shall be performed at least annually.*

*Measures for user identification and authorisation*

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*
- *The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.*
- *Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.*
- *The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.*

*Measures for the protection of data during transmission*

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*

## OFFICIAL

- The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.
- Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.
- The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.

### Measures for the protection of data during storage

- All corporate endpoint devices/laptops are encrypted using NIST standard encryption algorithms at the disk or volume level leveraging technologies incorporated in the operating system (e.g. Bitlocker and Filevault using AES-128 bit encryption or higher);
- Application credentials and service accounts are encrypted and stored in centrally managed solutions. (e.g. Hashicorp Vault, LastPass, etc.)
- Amazon RDS Databases are encrypted at the database level using NIST AES standard of 128 bit encryption or higher.
- Pluralsight plans to enhance encryption at rest strategies in AWS by the end of 2021 by further encrypting all Amazon EBS volumes and all customer data stored in Amazon S3 buckets.
- Pluralsight does not ever store credit card information in our data stores; rather, Pluralsight utilizes third-party services, which are PCI-certified and implement industry data security standards appropriate for that data classification, to manage all confidential subscription and billing information.
- The Pluralsight platform leverages the bcrypt hashing algorithm for all individual customer passwords and only ever stores the hashed output of that computation.

### Measures for ensuring physical security of locations at which personal data are processed

- Customer data is housed in AWS where their physical security controls are leveraged ([www.aws.amazon.com/security](http://www.aws.amazon.com/security) & [www.aws.amazon.com/compliance](http://www.aws.amazon.com/compliance))
- Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required that Pluralsight reviews Amazon Web Services (AWS) SOC II which provides appropriate assurance of AWS' physical security practices.

### Measures for ensuring events logging

- Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required that Pluralsight has appropriate event logging practices in place.
- All critical devices, systems, datastores, and applications have event logging enabled. Logging events must contain what occurred, who or what caused the event, when the event occurred (i.e. timestamp), and the associated system applications or data affected by the events.
- Where possible, the following system, datastore, and application types of events should be logged:
  - All authentication events (success and fail)
  - Account or role creation, modification, or deletion
  - Changes to system or application configuration
  - All alerts raised by the access control system
  - Administrator or operator activities
- Centrally collected event logs from systems, datastores, and applications. Access to centrally collected event logs is controlled by these teams and limited to "need to know" scenarios. Centrally collected event logs are retained for a period of no less than 12 months.

### Measures for ensuring system configuration, including default configuration

- Configuration Standards such as an Implementation Checklist and Operating Procedures are in place for system components. This also includes a description of any manual or automated tasks for installation and maintenance, backup, error handling, system restart and recovery procedures, logging and monitoring methods.
- Default vendor passwords must be changed after the installation of systems or software and before system or software is used in production.

### Measures for internal IT and IT security governance and management

## OFFICIAL

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Personal data is protected with least privilege access and handled with appropriate operational procedures.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Laptops are necessary to conduct business tasks and are provided and centrally managed by IT. Other personally-owned mobile devices, such as smartphones, that are not owned by Pluralsight must adhere to our Mobile Device Policy & Standard (MDM). To protect mobile devices and business related data, the IT team is responsible for the implementation of technical security measures. Additionally, every team member is responsible to ensure that mobile devices accessing Pluralsight data comply with the following requirements:*
  - *Access to devices must be authenticated (including a PIN on mobile devices).*
  - *The device is encrypted.*
  - *Anti-malware software and definitions are updated automatically.*

*The IT team and Information Security team have the right to control information on mobile devices and forensically examine the device believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.*

- *Team members are permitted to carry personal smartphones or tablets with them to corporate offices. The accessing, processing, copying, or taking pictures of business related data and documents is strictly prohibited.*
- *Team members shall be positively identified, authorized, and authenticated before they are granted access to company information resources.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Access to information resources shall be controlled through a defined and managed process which addresses authorizing, modifying, and revoking access, and which includes a periodic review of information system privileges.*
- *A user enrollment process shall be created, documented, implemented, and maintained on a regular basis.*
- *Each user shall be uniquely identified.*
- *Each user requiring access to Pluralsight's information assets above the standard access for their job function shall submit a request*
- *User access requests shall be retained as required by business and regulatory needs.*
- *Information resources and network services shall not be accessible to users unless the user has been explicitly authorized and granted permission to access the resource or service.*
- *The allocation and use of privileges shall be restricted and managed.*
- *User privileges shall be tracked at the application level and each user's profile (identity, access, privileges, and authorization) recorded and managed to prevent misuse of resources.*
- *Authentication tokens (i.e., passwords) and keys for privileged users must be rotated upon termination.*
- *User access and privileges shall be reviewed through a defined process.*
- *Reviews of non-administrative and administrative user access rights shall be performed at least annually.*
- *Change requests serve as a "notice" to others within Pluralsight regarding proposed alterations to the IT environment. Change requests may come from a variety of individuals within the company and are necessary for effective tracking and information management. Requests are initiated by logging a request for change on the IT change request system.*
- *Change authorization is performed by the Pluralsight IT and Security teams.*
- *A Change review will occur following the implementation of the change into the production environment. This function may be performed by a variety of personnel, but traditionally the function is best performed by those performing the actual distribution functions, or others who may be most familiar with the performance of the production environment.*
- *All Pluralsight team members are trained and educated on internet browsing and email best practices to help protect against malware, phishing, and ransomware. Team members must be attentive to indications of a compromise and must contact the IT team immediately if a compromise is suspected.*

OFFICIAL

## OFFICIAL

- *The IT and Operations teams are responsible for implementing anti-malware capabilities. They establish a patch management process for systems they support and a procedure to remain aware of new vulnerabilities. These teams are also responsible for ensuring the following take place:*
- *All Windows and MacOS systems, as well as Linux systems have approved anti-malware software installed and operating.*
- *Anti-malware is centrally administered by the IT and Operations teams.*
- *Anti-malware is centrally monitored by the Information Security team.*
- *Anti-malware definition files and/or updates are downloaded and installed automatically.*
- *Anti-malware software is configured to scan all files before being accessed and/or written to disk.*
- *Anti-malware is configured to clean, quarantine, or delete any infected file.*
- *Anti-malware software is enabled at system startup and configured to only be disabled by system administrators.*
- *Anti-malware software is capable of generating audit logs and is enabled at all times.*
- *Operational software is only installed, deployed, maintained, and tested by the IT or Operations teams and a configuration control system is deployed to manage and document authorized software, applications, or libraries.*
- *The IT and Operations teams are responsible for the management of the Pluralsight business and product networks, respectively. This includes the administration and monitoring of those networks for the purposes of security and availability. All remote network level access and administration is restricted by firewall authentication. Complete network level access is only granted to the IT and Operations teams. All requests for access and network changes follow the change management process.*
- *Networks, including the components which comprise them, shall be managed and controlled to limit threats and vulnerabilities.*
- *Network controls shall ensure the protection and security of the information processing services and applications dependent on the network infrastructure.*
- *Network services agreements, whether in-house or outsourced, shall include the following provisions:*
- *Security features and requirements.*
- *Service level agreements.*
- *Specified responsibility for managing security requirements on both sides of the service delivery process.*
- *Groups of information services, users, and information systems shall be segregated on the network.*
- *Grouping shall be determined by business function, information classification, the Access Control Policy, and user access requirements.*
- *The IT and Operations teams ensure that Pluralsight networks are segregated (using authentication, physical and logical access restrictions) from each other using network ACLS, firewalls, VPNs, security groups, etc. They establish specific segments for each office location, guest wireless, team member wireless, development/test, stage, and production environments. Team member wireless access is, at a minimum, WPA2 Enterprise and requires unique credentials for each user.*
- *The Information Security team assesses each environment at least annually for risks.*

### *Measures for certification/assurance of processes and products*

- *Disaster Recovery Testing is conducted quarterly*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

### *Measures for ensuring data minimisation*

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Personal data is protected with least privilege access and handled with appropriate operational procedures.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*

*Measures for ensuring data quality*

- *Disaster Recovery Testing is conducted quarterly.*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted. Data validation inputs are also reviewed as part of the ISO 27001 certification.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

*Measures for ensuring limited data retention*

- *Data protection laws require that personal data not be retained for longer than is necessary for the purpose for which it is processed.*
- *Records must not be retained beyond the period indicated in the Records Retention Schedule unless the record is identified as information subject to a litigation hold or other valid business reason. If you are uncertain as to when a record can be destroyed, you can reach out to the Legal Department for guidance.*
- *Erasure Requests: Pluralsight has added a "delete my account" feature, thus facilitating learner requests to be forgotten. When a learner deletes their account, all data associated with that account in the product will no longer be identifiable to a natural person.*

*Measures for ensuring accountability*

- *Disaster Recovery Testing is conducted quarterly.*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

*Measures for allowing data portability and ensuring erasure*

- *Erasure Requests: Pluralsight has added a "delete my account" feature, thus facilitating learner requests to be forgotten. When a learner deletes their account, all data associated with that account in the product will no longer be identifiable to a natural person.*

*Measures for assisting the data exporter with data subject access requests*

***Data importer will assist data exporter in meeting its obligations under the GDPR by either (i) providing Customer the ability within the Platform to access, correct or delete personal data or restrict its processing; or (ii) if such functionality is not available within the Platform, make personal data available to data exporter, or as applicable, make such corrections, deletions, or restrictions on data exporter's behalf.***

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter***

***Pluralsight contractually binds its sub-processors to technical and organizational measures substantially equivalent to those to which Pluralsight has committed herein.***

## Addendum II – International Data Transfer Addendum

### International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

#### PART 1 TABLES

Table 1: Parties

Start Date	The Start Date for this Addendum shall coincide with the start date of each Agreement between the Parties.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
	The Exporter is the Customer as identified in Annex I.A. of the EU SCCs found in Addendum I.	The Importer is Pluralsight, LLC.
Parties Details	Exporters' details are as set forth in Annex I.A. of the EU SCCs found in Addendum I.	Importer's details are as set forth in Annex I.A. of the EU SCCs found in Addendum I.
Key Contact	Exporters' Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I.	Importer's Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I.
Signature	The Parties agree that their signatures affixed to the EU SCCs in Annex I.A. of Addendum I shall serve to legally bind the Parties to this Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		<input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:      Reference:      Other Identifier:									
		<input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:									
Module	Module in Operation	Clause 7 Docking Clause	Clause 11 (Option)	Clause 9 a (Prior Authorisation / General Authorisation)	Clause 9 a (Time Period)	Is personal data received from the Importer combined with personal data collected by the Exporter					
1	No										
2	Yes						No	No	Yes	30 Business Days	
3	No										
4	No										

Table 3: Appendix Information

**OFFICIAL**

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	Parties are as set forth in Annex I.A. of the EU SCCs found in Addendum I.
Annex 1B: Description of Transfer:	Description of Transfer is as set forth in Annex I.B. of the EU SCCs found in Addendum I.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	TOMs are as set forth in Annex II to the EU SCCs found in Addendum I.
Annex III: List of Sub processors (Modules 2 and 3 only):	Sub processors are as set forth in Call-off Contract.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes.	Which Parties may end this Addendum as set out in Section 19:
	<input type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> Neither Party. Clause 18 will apply in the event the Approved Addendum changes in accordance therewith.

**PART 2: MANDATORY CLAUSES**

Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects’ rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section Error! Reference source not found..

**OFFICIAL**

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

**OFFICIAL**

- b Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
- a References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
  - b In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
  - c Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
  - d Not applicable. Intentionally left blank;
  - e Clause 8.8(i) of Module 2 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
  - f References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g References to Regulation (EU) 2018/1725 are removed;
  - h References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
  - i Not applicable. Intentionally left blank;
  - j Clause 13(a) and Part C of Annex I are not used;
  - k The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
  - l In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
  - m Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;
  - n Clause 18 is replaced with:

**OFFICIAL**

**OFFICIAL**

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

- o The footnotes to the Approved EU SCCs do not form part of the Addendum.

Amendments to this Addendum

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a Makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and / or
  - b Reflects changes to the UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

- 19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate, and demonstrable increase in:
  - a Its direct costs of performing its obligations under the Addendum; and / or
  - b Its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

- 20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
-------------------	---

# **Pluralsight Service Definition Document for G-Cloud 13 Framework Buyers**

Pluralsight Skills & Pluralsight Professional Services for  
G-Cloud 13 - May 2022

# Table of Contents

## Contents

Introduction	5
Pluralsight Skills	5
Who We Are	5
Slowing Down is your Biggest Threat	5
Time isn't on anyone's Side	5
The Service	6
The Clarity You Need To Lead	6
The Skills To Move Faster	6
Succeed Ahead Of Schedule	6
Pluralsight for Developers	7
Are you keeping pace?	7
Lead the pack with Pluralsight	7
Empower critical development roles	7
Develop technical competencies	7
Assess skills in technologies	7
Pluralsight for Information & Cyber Security	8
Are you doing enough?	8
Stay two steps ahead with Pluralsight	8
Support critical security roles	8
Develop key skills	8
Help your team prepare for certifications	8
Pluralsight for Cloud	9
When It Comes To Cloud Strategies, There's No Such Thing As One Size Fits All.	9
Gain Confidence On The Fundamentals	9
Upskill Teams Into Modern Cloud Roles	9
Execute On Your Cloud Strategy	9
Drive Towards Cloud Maturity Faster	9
Empower critical development roles	9

Develop key skills:	9
Benefits and Outcomes	10
Platform Capabilities	11
Iris	11
Pluralsight IQ	11
Role IQ	11
Our content	11
Our authors	11
Paths	11
Channels	12
Skill Assessments	12
Certification Practice Exams	12
Mobile, Desktop, and Streaming Apps	12
Advanced Skills Analytics	12
Advanced Channels Analytics	13
Enterprise Plan Overview	14
Learner Features	14
Leader Features	14
Professional Services	15
ProServ Onboarding †	15
Skills Strategy	15
Integrations	16
ProServ Integrations	16
Self Service Onboarding (Non-Chargeable)	16
Learner Self Service Onboarding (Non-Chargeable)	17
Self Service Skills Admin & Manager (Non-Chargeable)	17
Licensing, Ordering and Invoicing	18
Pluralsight Service Level Agreement	19
Technical Requirements, Integration and Support FAQ	21
What software do I need to have installed on my computer?	21
What browsers do you support?	21

Do you use Cookies?	21
Do you have mobile and offline options?	21
What integration options do you have?	21
How do I contact Support?	22
Offboarding	22
Exit Plan	22

# Introduction

## Pluralsight Skills

This is the service definition document for the Pluralsight Skills G-Cloud provision of services.

Pluralsight is the technology skills development platform for organisation's that need to enhance the expertise of their technologists and deliver key innovations on time, on budget and securely. With Pluralsight Skills, you can evaluate the technical abilities of your teams, align learning to key business objectives, and close skills gaps in critical areas like cloud, mobile, security and data.

Pluralsight is unique in its ability to help CIO's and CTOs develop technology skills at scale. Only Pluralsight Skills enables organisation's to measure their technology skills, deliver personalised learning recommendations, create an organisational skills index and inventory and upskill teams into modern tech roles. Unlike traditional online learning solutions, Pluralsight Skills combines the platform, content and services that the Public Sector, Government Departments, and ALBs need to deliver innovation faster.

Pluralsight has over 7,500 on-demand courses as well as, guides and skills assessments in the areas of Software Development, IT Ops, Data, Cloud, Mobile, Creative, Digital Engineering and Cyber Security.

Below you will find the services which we are proposing together with the supporting technologies.

## Who We Are

In the digital age, technology teams are only as successful as their skills are relevant. This is even more vital in the Public sector with retention of talent and providing opportunities for upskilling on leading edge technologies at the forefront of a leader's minds.

## Slowing Down is your Biggest Threat

The Public Sector is under pressure to become more agile, protect against rising security threats and continuously deliver innovation to their respective organisations and the public. Leaders have no idea what teams are capable of or how best to leverage their expertise to deliver on their technology strategy. Mobilising teams around that strategy can be a painfully slow process, and all the while employees' skills are becoming less relevant as technology evolves faster and faster.

## Time isn't on anyone's Side

The average lifespan of Fortune 500 companies will be cut in half to just 12 years by 2027\*.

By leveraging Pluralsight Skills technology skills platform, you can get out of reactive mode. Upskill teams into modern roles, put the right people on the right projects and ship faster than ever.

It's how you develop skills at scale.

\*Innosight 2018 Corporate Longevity Briefing

## The Service

With Pluralsight's technology skills platform, you can align your technology strategy to a skills strategy that moves you forward faster.

### The Clarity You Need To Lead

- Index the skills of your entire organisation with Skill IQ
- Upskill employees into modern tech roles with Role IQ
- Build fluid teams that meet objectives with advanced analytics

### The Skills To Move Faster

- Learn from our network of 1,500+ authorities on cloud, microservices, machine learning, security, Agile and more
- Develop and apply skills faster with personalised recommendations from Iris
- Accelerate your skills strategy with the help of our powerful Professional Services

### Succeed Ahead Of Schedule

- Become more reliable, adaptable, scalable and secure
- Speed up release cycles
- Cut costs and improve efficiency

# 295%

ROI with <6 months payback period\*

# \$11.3M

In savings from faster product development \*

*\*Source: The Total Economic Impact™ Of Pluralsight, an October 2017 commissioned study conducted by Forrester Consulting on behalf of Pluralsight*

## Pluralsight for Developers

Pluralsight Skills technology learning platform helps developers become skilled in the languages, tools and frameworks that power innovative product experiences.

### Are you keeping pace?

Technology is fundamentally changing the way organisations operate and deliver value to customers. To keep pace, it's imperative to invest in the skills of your development teams. Ask yourself the following:

- Will our current tech stack enable us to meet future customer needs?
- How quickly does our team push new code?
- What percent of time is spent maintaining projects vs. building new ones?
- Do we have the talent to deliver winning mobile, web, and cloud experiences?

### Lead the pack with Pluralsight

Establish an advantage by empowering your teams to learn and improve with Pluralsight—the leading platform for developing technology skills at scale.

#### Empower critical development roles

- Web
- Application
- Mobile
- Database
- Cloud
- Full stack
- Front end
- Back end

#### Develop technical competencies

- Continuous integration
- Enterprise architecture
- Agile development
- API integration

#### Assess skills in technologies

- C#
- JavaScript
- Python
- Java
- HTML 5
- Angular
- C++
- PowerShell
- MySQL
- React
- ASP.NET
- CSS

Empower your development teams to build innovative product experiences.

Learn more: [www.pluralsight.com/browse/software-development](http://www.pluralsight.com/browse/software-development)

## Pluralsight for Information & Cyber Security

With Pluralsight Skills technology learning platform, you can empower your entire organisation to recognize, understand and react to rising security risks.

### Are you doing enough?

If your teams have held off security breaches up until now, it's time to knock on wood. It's no longer about if a security breach will happen, but when and how hard your data will be hit. Ask yourself these questions:

- What is your number one security pain point?
- How do you ensure new security hires have the right skills?
- Have any of the recent industry breaches impacted your need to enhance your security expertise?

### Stay two steps ahead with Pluralsight

Give your organisation a fighting chance with content authored by industry experts who have real-world experience in both offensive and defensive security.

### Support critical security roles

- Penetration Tester
- SOC/Security Analyst
- Incident Responder
- Digital Forensics Analyst/Examiner
- Information Systems Auditor
- Security Engineer
- Security Architect

### Develop key skills

- Digital Forensics and Incident Response
- Penetration Testing
- Security Coding
- Security Assessments
- Security Compliance

### Help your team prepare for certifications

- CompTIA Security+ (Exam SYO-401)
- CompTIA Security+ (Exam SYO-501)
- CompTIA Security Practitioner (CASP) (Exam CAS-002)
- CompTIA Cybersecurity Analyst (CSA+)
- Ethical Hacking (CEH Prep)
- Information Systems Auditor (CISA Prep)
- Risk Management and Information Systems Control (CRISC Prep)
- CISSP
- SSCP

Empower your entire org to safeguard against security threats.

Learn more: [www.pluralsight.com/browse/information-cyber-security](https://www.pluralsight.com/browse/information-cyber-security)

# Pluralsight for Cloud

## When It Comes To Cloud Strategies, There's No Such Thing As One Size Fits All.

That's why organisations need a single skills development platform capable of building and evolving their cloud strategy—no matter their maturity state or provider. By partnering with Microsoft Azure, AWS and Google Cloud, Pluralsight is the only platform that offers broad and deep skills coverage for any cloud strategy.

### Gain Confidence On The Fundamentals

From app development, storage, analytics and virtualization—getting a strong start is important. Build on the basics with cloud fundamentals courses, identify gaps with skill assessments and inform multi-cloud strategies with analytics that put the right people on the right cloud initiatives.

### Upskill Teams Into Modern Cloud Roles

A cloud strategy requires teams to execute at different speeds, fundamentally changing the way they operate. Pluralsight gives you the ability to continually evolve skills, roles and organisational designs to ensure your teams are as agile and scalable as the cloud itself.

### Execute On Your Cloud Strategy

Develop skills to distribute workloads across multiple public cloud providers to reduce the risk of a single point of failure and take advantage of each provider's unique platform integrations, features and capabilities.

### Drive Towards Cloud Maturity Faster

Create a strategy for migrating applications and data, as well as moving existing applications to the cloud. Build new applications with a cloud-first mindset using containers and microservices. And, give your teams the ability to provision, configure, deploy, monitor and decommission environments faster for improved development.

## Empower critical development roles

Key Partnerships include Google Cloud, Microsoft Azure and AWS amongst others.

- Cloud Architects
- Cloud Engineers
- Cloud Administrators
- Microsoft Azure, AWS and Google Cloud specific roles

### Develop key skills:

- Cloud fundamentals
- Cloud Infrastructure
- Cloud architecture and design
- IaaS, PaaS, SaaS
- Cloud platforms, including Microsoft Azure, AWS, and Google Cloud
- Virtualization, networking, and operations
- Operating systems and stacks
- Microservices
- DevOps
- Containers
- Continuous Integration and Deployment
- Data centre management and databases

## Benefits and Outcomes

- Faster product development value - Employees may gain new capabilities, ideas, and innovations when they use Pluralsight, resulting in new products created and launched faster.
- Cost avoidance: retaining employees - Employee opportunities for enrichment via Pluralsight might lead to goodwill and greater attachment to the organisation; more employees are retained.
- Cost avoidance: travel & tuition - Using Pluralsight Skills, fewer employees might travel to offsite courses and conferences, saving the company travel and tuition costs.
- Cost avoidance: senior staff time at basic tech instruction - When Pluralsight is used for basic technical instruction, senior engineers can shift more time from instruction to their main jobs.
- Cost avoidance: external instructors - Pluralsight Skills closes the gap for experienced new hires to acquire the company-specific technical skills needed to reach productivity.
- Faster onboarding of experienced new hires - Pluralsight closes the gap for experienced new hires to acquire the company-specific technical skills needed to reach productivity.
- Faster onboarding of junior developers - Using Pluralsight Skills for tech orientation of junior professionals might result in faster ramp up to full productivity specific to their assigned teams.

Departments and Organisations will achieve these benefits with the following Pluralsight capabilities:

- Administer assessments to assess technical readiness, then view your team's proficiency relative to their role and the business objective at hand
- Identify & quantify skill gaps, and then prescribe learning that fills skills gaps needed to meet business objectives
- Learn from an exclusive list of vetted platform experts with proven ability to transfer knowledge, thereby acquiring the skills to set technology standards rather than chase them
- Modernise product development processes by completing courses on the most current development methods and implementing them across the organisation
- Give employees an efficient way to start learning a new technology and put what they've learned into practice
- Onboard employees quickly with a cost-effective, on-demand skills platform that scales across technology teams
- Virtually access the foremost technology experts to understand emerging technologies, while you could simultaneously assess current skills, and create customised learning paths to fill the gaps

## Platform Capabilities

### Iris

Iris is a new way to measure and evolve technology skills. This artificial intelligence powers our assessment algorithm and guides learners to the skills your business needs now. The more they learn about technology, the more Iris learns about their skills. Iris uses data to create a smarter, personalised skill development journey. It is the science behind our platform.

Iris is disrupting skill development for individuals, businesses and the world. With Iris, learners can validate their current proficiency and feel confident they know where to focus on improving their skills. Pluralsight Skills is at the centre of the tech skills ecosystem and the future of a new world for technology certifications. And it starts with the ability to measure an individual's skills.

### Pluralsight IQ

This is your Iris Quotient. Individuals can measure their skills in as little as 5 minutes and 20 questions. Each result includes a Skill IQ, a skill level, a percentile rating for the skill area/technology and a date of verification. People who complete our assessments get an "Iris Quotient," or IQ--it's a hard number from 0 to 300 that tells them exactly where they stand. It benchmarks their skill levels against the workforce and gives them a novice, proficient or expert status.

### Role IQ

We also offer Role IQ, which shows you and your team members the skills you need to succeed, where skills gaps exist and what you need to work on to reach role mastery. Leaders can customise roles to fit specific business needs and help everyone build the right skills.

### Our content

Skill up with thousands of on-demand video courses, teaching the most high-demand technologies, tools, processes and best practices across the IT industry. Inform your technology strategy with courses authored by trusted industry experts. Enable your teams to adapt quickly and create the future-focused technology needed by your company.

With interactive courses and projects, your team can practice and apply new skills in risk-free environments and get guided feedback along the way. They'll have confidence their skills are ready for critical projects.

### Our authors

Our author ecosystem consists of hundreds of proven experts who not only have the passion, but have the teaching skills to spread their knowledge to the world. Whether you're a novice or an expert, our authors provide the content needed to take your skills to the next level.

On average, we only publish three out of every 1,000 content proposals we receive. Why? To ensure every course we publish meets the quality standards our customers demand.

### Paths

It can be tough to know where to start learning. Paths combine specific courses and tools into one experience to teach you any given skill from start to finish. Paths are aligned to an individual's knowledge level, to help you and your team develop the right skills in the right order.

Our paths combine courses and tools into one experience so you can effectively learn a new skill in the right order. Individuals can measure knowledge and skill development over time by completing associated learning checks, skill assessments and certification practice exams.

## Channels

Channels are an intuitive way to organise and share Pluralsight Skills content so you can reach your learning goals and business objectives more effectively. Create channels to curate content for your own learning, for team development or to share learning journeys with the world.

Channels empower operational leaders to curate custom learning plans to address desired outcomes. With channels, you can align learning to your key business objectives and guide teams towards skills that will make them successful.

## Skill Assessments

Get an accurate read on your team's skills. In as little as five minutes, you and your team members can see exactly where your skills stand on dozens of technologies, allowing you to pinpoint areas of expertise and improvement. Skill assessments measure your knowledge of a particular skill and gives you an objective rating of where you stand in relation to other technologists around the world with your Skill IQ.

## Certification Practice Exams

Whether you're looking to prepare for your own certifications or are encouraging employees to get certified, your road to exam-readiness starts with Pluralsight. You and your team can prepare for exams to improve the likelihood of passing your certification exams—saving hundreds, if not thousands of dollars.

Once you're ready to take a practice exam, you can conveniently navigate to Kaplan right from the certification path. Learn from different test modes – including optimised tests, practice tests and flashcards – to assess your readiness. You can also view incorrect answers with detailed explanations to learn as you go. After completing practice exams, you can see your exam history and results right within Pluralsight.

## Mobile, Desktop, and Streaming Apps

Make your learning fit your schedule with an on-demand platform that's ready whenever and wherever you are. Whether you're taking a break at work, in the comfort of your home or on your commute, you can pick up exactly where you left off and keep learning with Pluralsight.

Easily stream or download training on your iPhone, iPad, Android phone or tablet. No internet? No problem. Download courses and learn with offline player apps for Windows (requires Windows 7 and up) and Mac (requires OS X 10.11 and up). You can extend your learning to the big screen with apps for Apple TV, Amazon Fire TV and Roku.

## Advanced Skills Analytics

With advanced skills analytics, you can see the strengths and weaknesses of your team with unmatched clarity. Individual and topic-level insights help you find opportunities for growth, discover hidden talent, and put the right people on the right projects.

Skills shouldn't be subjective. View quantified skill levels for individuals across your entire organisation, so you can identify top performers and help others close the gap. Check out your team's distribution of skills by topic. Quickly identify knowledge gaps and prioritise team learning. You can even view skill progress over time.

CIOs, CTOs and other senior technology leaders can make informed decisions based on deep, empirical data regarding proficiency levels and ensure projects are serviced by the right resources in a timely manner. Where there are skills gaps, these can be addressed and eliminated quickly, leading to more effective and efficient delivery.

## Advanced Channels Analytics

Channels empower operational leaders to curate custom learning plans to address desired outcomes. Advanced channels analytics gives you visibility into how colleagues are progressing through these custom paths, so you can help them stay on track.

Advanced channels analytics is how technology leaders understand how close (or far) individuals are from reaching their learning goals, through analytics demonstrating completion percentage and last activity. This capability enables you to guide learning journeys, to ensure the highest probability of your employees improving their capabilities in mission critical skills.

# Enterprise Plan Overview

## Learner Features

- **COURSE LIBRARY.** Upskill your employees with thousands of expert-led courses across hundreds of topics.
- **PATHS.** Build proficiency by knowing which courses to watch in which order, with course work curated by experts.
- **CHANNELS.** Combine sections of different courses or paths to create a custom skill development plan for your team aligned to your business objectives.
- **SKILL IQ.** Measure and index your team's technology proficiency with quick, adaptive skill assessments.
- **ROLE IQ.** Benchmark proficiency across all your technical roles to see if your employees have the skills they need to succeed at their jobs.
- **COURSE COMPLETION CERTIFICATES.** Get verification that a course has fully been completed.
- **COURSE LEARNING CHECKS.** Test retention of course material with short, self-paced quizzes.
- **COURSE DISCUSSIONS.** Employees can engage with peers and the expert author in a community dedicated to each course.
- **CERTIFICATION PRACTICE EXAMS.** Prepare for professional certifications with industry-leading practice exams.
- **EXERCISE FILES.** Course slides, instructor notes, source code and more are available for download.
- **MOBILE, TV APPS & OFFLINE VIEWING.**
- Employees can learn anytime, anywhere with mobile and desktop apps that allow for offline viewing.
- **EMAIL AND PHONE SUPPORT.** Questions? We're here for you. Email: [Support@pluralsight.com](mailto:Support@pluralsight.com), available 24/7. Phone: (801) 784-9007, available M-F from 8am-5pm MST. Additional phone support available from your Account Executive M-F from 9am-6pm GMT.

## Leader Features

- **TEAM MANAGEMENT.** Add, update and remove users and view user logs.
  - **ADVANCED ROLES ANALYTICS.** Get an individual view of role proficiency so you know which team members are prepared to tackle your key objectives.
  - **ROLE CUSTOMIZATION.** Select specific skills to design custom roles that are aligned to your organisation's unique needs.
  - **ADVANCED SKILLS ANALYTICS.** Get unprecedented insight into skill proficiency across your organisation, including progress over time.
  - **ADVANCED CHANNELS ANALYTICS.** Measure progress towards business objectives by ensuring employees are completing content and courses.
  - **TREND ANALYTICS.** See which courses and subjects are popular and trending across your teams.
  - **USAGE ANALYTICS.** View usage, hours spent on skill development and a leaderboard of your top team members.
  - **API ACCESS.** Always have the latest data on how your team is using Pluralsight with APIs that include user data, and course usage and completions.
  - **DATA EXPORT.** Have the flexibility to create your own recurring reports and analysis.
- \*All per user products require an annual contract.

## Professional Services

Professional services are not included in the Licence fee

### ProServ Onboarding †

To really get the most out of your team's talents and reach your goals, you need a hyper-personalised skills development strategy integrated into your tech ecosystem. With ProServ Onboarding, you can kickstart your new skill development solution and start driving results.

Your assigned technical onboarding consultants and skills strategy experts uncover your most pressing technology initiatives and craft a skills and platform deployment strategy that allows you and your team to hit the ground running.

Through this engagement, you'll receive:

- An Assigned Technical Onboarding Consultant who will manage your Pluralsight onboarding experience
- An onsite onboarding workshop to plan your project and discover your business goals, technology job roles and technology stack
- Your technology strategy mapped to learning on the Pluralsight platform, implemented through channels
- Integrations into your technology ecosystem through SSO, APIs and data exports
- Enablement sessions, and best practices to help drive adoption, continuously improve your skills development program, and report on skill development
- Consistent check-ins to track progress

A ProServ Onboarding engagement is critical to getting your experience Pluralsight started on the right foot.  
† Subject to the Pluralsight Professional Services Terms and Conditions – Costs apply (see Pluralsight Pricing document)

### Skills Strategy

ProServ Skills Strategy † (Included in Onboarding package but can be purchased independently)

Through ProServ Skills Strategy, Pluralsight's Professional Services team provides ongoing consultative guidance to identify and eliminate skills gaps at scale. We begin by building an understanding of your desired outcomes, then our experts work with you to map out the skills and related systems, tools and topics your teams need to learn across all experience levels. Through ongoing virtual consultations, we help you deliver innovation faster and accomplish your strategic objectives.

Many of our customers are seeking much deeper assistance in understanding the roles, goals, and tech stacks that exist across a wide array of technology business units and then aligning learning to those. With ProServ Skills Strategy, you benefit from access to resources from our Professional Services organization, who will consult with any number of subject matter experts and technology leaders from your company, via virtual meetings, plus telephone conversations.

Through this engagement, you'll receive:

- A custom skills matrix that inventories the skills required to achieve your business objectives
- A custom mapping of your technology strategy to the Pluralsight platform
- Implementation of learning through Pluralsight channels
- Best practices to help drive adoption and continuous improvement
- One-time check-in to track progress

A ProServ Skills Strategy engagement is critical to establishing a true strategic partnership and effectively aligning the capabilities of our platform, to help deliver your desired outcomes, across all your technology teams.

† Subject to the Pluralsight Professional Services Terms and Conditions – Costs apply (see Pluralsight pricing document)

## Integrations

### ProServ Integrations

ProServ Integrations allow you to fully customize your Pluralsight experience and embed learning into your existing learning eco-system of systems and tools.

With custom integrations, you will:

- Remove roadblocks to give your team a streamlined and secure experience through Single Sign-on. SSO makes it easy to provision licences automatically, keep your team focused on learning, and protect your organization's security and privacy. You'll also lessen the administrative burden for your program managers. All attributes are passed across a federated connection on sign-in therefore data privacy is supported as no batch-files have to be exchanged.
- Have full clarity into how your team uses Pluralsight with APIs that include user data, course usage and course completions.
- Collect data your way with the ability to build custom, recurring reports and analysis.
- Build a one-stop-shop for skill development by combining data export with single sign-on to provide learners with a unified experience, integrating Pluralsight into any of the major learning management systems.

† Subject to the Pluralsight Professional Services Terms and Conditions – Costs apply (see Pluralsight pricing document)

## Self Service Onboarding (Non-Chargeable)

The standard offering consists of a comprehensive [Self Service offering](#).

Our guided self-serve onboarding covers all the basic areas for administration and learner onboarding. Below is a list of the main provision which is accessible via the help portal. Full access will be provided.

### Learner Self Service Onboarding (Non-Chargeable)

Full information can be seen on the [Get Started: Skills Learner Onboarding](#). The following sections are included:

- Get to Know Pluralsight Skills
- Accept your invitation and Set-up your Account
- Take your First Course
- Assess your Skills and Dive In
- Take the Platform with you – Anywhere
- What is my Role?
- How to make Skilling up a weekly habit

There are many learner videos, assisted and adaptive learning paths as well as much more.

### Self Service Skills Admin & Manager (Non-Chargeable)

The Plan Manager & Team leader has a comprehensive online self-service tutorial in the [Admin success center: Skills](#) to help you get the most out of your Pluralsight experience including:

- Get started
  - Lay the groundwork
  - Invite your team
- Drive learning and growth
  - Guide your team
  - Leverage analytics
  - Encourage learning
  - Know what's new
- Quick links
  - All resources

## Licensing, Ordering and Invoicing

Pluralsight provides access to its online technology skills platform on a 12-month subscription basis. The Buyer will obtain access to the Pluralsight Skills application for the number of individual subscriptions as specified in the Call-off Contract. The Buyer may add additional individual subscriptions during the initial term of the Call-off Contract by paying a licence fee prorated for the number of months remaining in such term.

With respect to a Call-off Contract and the individual User subscriptions set forth therein, a Buyer may transfer individual subscriptions to account for individuals who cease to be employed or otherwise change roles within Buyer's organisation during the subscription term, but such transfers may not exceed more than 10% of Buyer's aggregate licence count during any twelve-month period. Any other transfer(s) for any reason or no reason are prohibited.

Cost per Licence / 12 months Unlimited Access / Named User Licence

**Please refer to Pricing document for full details**

# Pluralsight Service Level Agreement

## 1. Availability

A. Uptime: The Platform shall be Available (as defined below) 99 percent (99.0%) of the time per month (24 x 7) except for planned maintenance downtime. "Available" shall be defined as the ability for Buyer to sign in, browse or search for a video course on the Platform, and play that course.

B. Uptime shall be calculated, in a given month, as the total number of minutes that the Platform, and all its functionality and features is Available during such month less the planned maintenance downtime divided by the total number of minutes during such month.

C. Any time that the Platform is unavailable for the following reasons shall not count towards the 99% uptime calculation:

- a fault on the Buyer's network or own equipment configuration.
- a fault/bug or other incident in the Buyer's software such as firmware, operating system, infrastructure software or the Buyer's own infrastructures or configuration of said infrastructures causing suspension of the Platform and/or hardware failure.
- incidents caused by any third party, where the third party is not appointed or under the direct control of Pluralsight.
- scheduled downtime for maintenance.
- third party network issues or suspensions.
- a cause beyond Pluralsight's reasonable control or
- downtime caused by the Buyer accessing the Platform over the internet, where the downtime is directly attributable to the public network itself.

## 2. Service Level Agreement / Response Times

Pluralsight shall provide support response to Platform inquiries under the following guidelines:

Type	Priority/Severity	Response Time Target	Restoration Time
Incident	1 – Critical/System outage	1 Hour	2 Hours
Incident	2 – High/Significant performance degradation	2 Hours	8 Hours
Incident	3 – Medium/Minor degradation of service	1 Business Day	48 Hours
Incident	4 – Low/Feature or "How To" request	5 Business Days	4 Weeks

## 3. Downtime Credits

If one or more interruptions in availability occur that collectively result in less than 99% availability during any single month, then at Buyer's request and provided Buyer is not in material breach of the Agreement, Pluralsight will grant Buyer additional Subscriber access, as set forth in the following table.

Network Availability Percentage of Month	Additional Customer Access
≥ 97.0% but < 99.0%	1 day
≥ 96.0% but < 97.0%	2 days
≥ 94.0% but < 96.0%	3 days
≥ 90.0% but < 94.0%	5 days
< 90%	10 days

## Technical Requirements, Integration and Support FAQ

### What software do I need to have installed on my computer?

- Our web player is based on HTML5, so it will not need any specific software installed on your computer. To use our HTML5 player, you'll need to be using a recent version of the browsers in the section below.
- Offline browsing of courses is available on several devices including desktops by downloading software, if desired. Please see the following website for details: [What mobile and offline systems does Pluralsight support?](#)

### What browsers do you support?

- Currently, to use Pluralsight Skills and watch Pluralsight Skills videos, we recommend using the following browsers and applications. **Please be sure to be on the latest version for each:**
- Windows 7, 8, 10 and MacOS\*:
  - o Microsoft Edge
  - o Firefox
  - o Chrome
  - o Safari
- **Browsers not supported:**
  - o Opera
  - o Internet Explorer

Pluralsight videos will work natively on Linux on a browser, since we stream videos through HTML5. Depending on your version of Linux, you might run into codec issues. The Pluralsight offline player does not work on Linux at this time.

\* Please note, over the life of the framework/contracts, support for versions of the above browsers and operating systems may change as new versions are introduced and others deprecated. The support website will provide the latest information on this topic.

### Do you use Cookies?

- We and our partners use cookies or similar technologies to make our site easier to use. We do not link the information we store in cookies to any personally identifiable information you submit while on our site. For full information on our use of cookies, please see our privacy policy on the Platform.
- Most web browsers automatically accept cookies, but if you prefer, you can change your browser to prevent that. We provide you with information about how to disable cookies in our privacy policy. However, you may not be able to take full advantage of our Site if you do so.

### Do you have mobile and offline options?

- We provide apps for iPhone & iPad, Android phone & Tablet, Desktop offline apps for windows and Mac, as well as for Amazon Fire TV Apple TV
- You can also cast to a Chromecast enabled device.

### What integration options do you have?

- Learning Management systems (LMS) integration
  - LTI 1.0 (Learning Technology Interoperability)
  - SAML 2.0 SSO – Single Sign On

- IdP app – OneLogin, Azure, Okta
- IdP or SP deep linking for embedded course-specific links
- IdP or SP catalogue linking for embedded catalogue links
- Application Programming Interface (API)
  - Extensive Course API & Reporting API
  - User management CRUD API (users, teams, channels, role IQs)
  - Please see our [API developer portal](#)
- We have whitepapers for integrations to popular systems such as SuccessFactors, Cornerstone, Degreed & Absorb. These and information for other integrations can be found on our [Professional Services webpage](#)

## How do I contact Support?

- 24/7 email ticketing system: [support@pluralsight.com](mailto:support@pluralsight.com)
- We have a telephone support available M-F 09:00 – 17:00 (GMT): see our [contact page](#)

## Offboarding

Pluralsight's Software as a Service (SaaS) Platform does not involve hosting or processing any of Buyer's business-critical information and Buyer is not utilizing Pluralsight's learning platform to perform any business operations, there is no data migration process upon contract termination.

Offboarding consists of:

- Plan managers can download Customer data at the end of the Call-off Contract Term.
- Upon Buyer request, a Plan can be deleted at the end of the Call-off Contract Term.

## Exit Plan

Pluralsight is a Software as a Service (SaaS) platform. SaaS platforms typically simplify a supplier's journey to another supplier. The most typical requirement for an organisation leaving the platform is to retain a copy of their data. When planning for the end of your contract there are some steps you can follow to retain your data:

- Plan Admins (managers) can download learner, course completion and skills data from within the Platform any time prior to contract end.
- Learners can download their notes and completion certificates.
- Plan Admins can remove learners from the Platform once all data has been downloaded.
- Subscriptions provided under a Call-off Contract, and all access to content provided on the Pluralsight platform based on such subscriptions, terminate simultaneously with contract termination.
- Moving data to another provider is the responsibility of the customer.

Please note: none of the above activities are mandatory, and may not be required when business plan subscriptions end.

# Thank you.

Pluralsight G-Cloud Sales  
[gcloudsales@pluralsight.com](mailto:gcloudsales@pluralsight.com)