

## 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	21
Schedule 1: Services	40
Schedule 2: Call-Off Contract Charges	45
Schedule 3: Collaboration Agreement	38
Schedule 4: Alternative Clauses	47
Schedule 5: Guarantee	48
Schedule 6: Glossary and Interpretations	49
Schedule 7: UK GDPR Information	58
Annex 1: Processing Personal Data	68

## 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>	403014234766519
<b>Call-Off Contract reference</b>	<i>C169808 Board Paper Management System</i>
<b>Call-Off Contract title</b>	Diligent Boards Portal
<b>Call-Off Contract description</b>	Licence to board meeting management software
<b>Start date</b>	02/05/2023
<b>Expiry date</b>	01/05/2025
<b>Call-Off Contract value</b>	<p>The initial value of this Call-Off Contract is GBP 28,000.00.</p> <p>The total maximum contract value, including the Extension Period and up to 50% optional growth, is GBP 63,000.00.</p>
<b>Charging method</b>	Annual Invoice
<b>Purchase order number</b>	

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

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

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

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

<b>From the Buyer</b>	NHS Business Services Authority <a href="tel:+441912325371">+441912325371</a> Stella House Street Goldcrest Way, Newburn Riverside Town Newcastle-Upon-Tyne Region Tyne & Wear Company Number: N/A
<b>To the Supplier</b>	Diligent Boardbooks Limited 0207 605 7438 25 Bedford Street, London, England, WC2E 9ES Company number: 06029195
<b>Together the 'Parties'</b>	

## Principal contact details

### For the Buyer:

Title:

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>02/05/2023</b> and is valid for <b>24 months</b> .
<b>Ending (termination)</b>	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least <b>90</b> Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of <b>30</b> days from the date of written notice for Ending without cause (as per clause 18.1).</p>
<b>Extension period</b>	<p>This Call-Off Contract can be extended by the Buyer for <b>one</b> period of up to 12 months, by giving the Supplier <b>1 month</b> written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>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</p>

	<p>Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p><a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a></p>
--	--

## Buyer Contractual Details

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

<b>G-Cloud Lot</b>	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> <li>• Lot 2: Cloud software</li> </ul>
<b>G-Cloud Services required</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> <li>• <b>Provision of the Diligent Boards software-as-a-service platform</b></li> <li>• <b>Support and account management of Buyer's use of the software-as-a-service platform</b></li> </ul>
<b>Additional Services</b>	<b>Training for all users to be provided.</b>
<b>Location</b>	The Services will be delivered to <b>locations throughout the United Kingdom via users' devices.</b>
<b>Quality Standards</b>	Not used.
<b>Technical Standards:</b>	The technical standards used as a requirement for this Call-Off Contract are <b>ISO27001</b>
<b>Service level agreement:</b>	<p>The service level and availability criteria required for this Call-Off Contract are as follows:</p> <p><b>DILIGENT BOARDS</b></p>

## **SERVICE LEVEL COMMITMENT**

### **Scope**

The following describes the minimum standards for availability of each of the below listed software-as-a-service offerings (as currently identified by Diligent) integrated into Diligent Boards™ (provided that Client has purchased access to such software-as-a-service offerings):

1. Diligent Boards;
2. Secure Meeting Workflow;
3. Secure File Sharing;
4. Diligent Minutes;
5. Messenger;
6. D&O Questionnaires; and
7. Evaluations Questionnaires.

This Exhibit does not apply to any other Diligent Services, including, for the avoidance of doubt, Content Services (where defined in the Agreement).

### **System Availability**

The Diligent Service will be available at least 99.5% of the time in any calendar month. Availability is determined by dividing the duration of "Service-Affecting Outages" by the total number of minutes in a calendar month and subtracting the resulting decimal number from 1.000. A Service-Affecting Outage shall be deemed to have occurred when the Diligent Boards Site is not available to Client except that outage time resulting from any of the following causes shall not be considered when determining the percentage of Availability:

1. Outages caused by failure in Client's operating environment (including Client's connectivity to the Diligent Service);
2. Outages for scheduled maintenance provided that such maintenance is scheduled during the hours of 10PM Friday – 4AM Saturday and/or 10PM Saturday – 4AM Sunday (based on the local time zone of the data center where Client Data is hosted). Diligent Service maintenance is ordinarily carried out so that it will not interfere with the availability of the Diligent Service. Diligent may revise the times at which scheduled maintenance may be performed by providing Client with at least thirty (30) days prior written notice of such revision.

	<p>3. Outages for emergency maintenance that Diligent determines is reasonably necessary;</p> <p>4. Outages that occur as a result of a Force Majeure Event; and</p> <p>5. Outages during a transition to the disaster recovery site following a disaster.</p> <p><b><u>System Availability Credits</u></b></p> <p>If the system level availability is between:</p> <p class="list-item-l1">(a) Ninety-nine and forty-nine hundredths percent (99.49%) to ninety-five percent (95%) in any given calendar month, Client shall receive a credit equal to ten percent (10%) of that month's Subscription Fees, being 1/12 of the annual Subscription Fee;</p> <p class="list-item-l1">(b) Ninety-four and nine tenths percent (94.9%) and below in any given calendar month, Client shall receive a credit equal to twenty-five percent (25%) of that month's Subscription Fees, being 1/12 of the annual Subscription Fee.</p> <p>The above listed system availability credits in subparagraphs (a) and (b) shall only be available to Client to the extent that Client has paid the Subscription Fees for the applicable software-as-a-service offerings identified under "Scope" of this Exhibit in accordance with the terms of the Agreement.</p> <p>If Diligent fails to reach the 99.5% level in three of any twelve consecutive calendar months Client shall have the option to terminate this Agreement per the terms and conditions governing this Agreement.</p> <p>If a Service-Affecting Outage occurs, Diligent will promptly respond upon receipt of notice from the Client. Diligent will attempt to achieve resolution of the Service-Affecting Outage as soon as possible but in no event longer than eight (8) hours from receipt of notice. The foregoing notwithstanding, in the event a software fix is required, this could take up to forty-eight (48) hours to implement, but this would be a rare occurrence. In such event, a work-around will be implemented, pending the software fix.</p> <p>The following reflects the escalation within the Diligent organization of a Service-Affecting Outage depending upon the time expired since receipt of notice:</p> <p>1 hour without resolution – Escalated to Director, Production Operations</p> <p>2 hours without resolution – Escalated to SVP, Production Operations</p> <p>3 hours without resolution – Escalated to CTO</p>
--	---

	<p>5 hours without resolution – Escalated to CEO</p> <p>This Exhibit sets forth Client's sole remedy for a failure in any month to meet the 99.5% system availability.</p>
<b>Onboarding</b>	<p>The onboarding plan for this Call-Off Contract is as follows:</p> <p><b><u>DILIGENT BOARDS IMPLEMENTATION PLAN</u></b></p> <p><b><u>Online Access</u></b></p> <p>The proposed implementation schedule below is a sample for planning purposes and will be further detailed and tailored to Client's unique requirements as Diligent gains a better understanding of Client's requirements. Implementation and training can begin within one week of Diligent's receipt of User surveys.</p> <p>The implementation process begins with a kick-off meeting at which the Client's team agrees on dates, timelines, and contact persons. Diligent recommends that administrative training be divided into two or three one-hour sessions, over a period of 2 -3 weeks. This ensures that Users have plenty of opportunity to learn at their own pace.</p> <p><b>PHASE 1      SITE LAUNCH</b></p> <p>During Phase 1, Client begins using the site for all boardbook production, realizing an immediate return on investment by streamlining the book assembly and approval process. An electronic platform is established for "rolling out" the Diligent Service to board members during Phase 2.</p> <p><b>Week 1 – 2      Kick-off Meeting</b></p> <p>Diligent introduces the account management team, establishes key milestones and reviews the Client's current board prep workflow and approval process.</p> <p>Client completes and returns User survey with list of authorised Users, access rights and site configuration requirements including password policy definitions and lists of client contacts.</p> <p>Boards Site is built and User accounts are created.</p>



## **Week 2 - 4**

Initial Training Sessions executed for Administrative Team

Client's first board book is produced using material from previous meeting – creating the first archival board book.

Production of Client's Information and board calendar begins.

Administrator manuals provided to internal Users.

Production begins for Client's board books for the first board meeting.

Board books are printed using Diligent's "Print Book" feature and distributed via conventional methods.

## **Week 3 – 6 Follow-up Admin Training Sessions Scheduled for Advanced Functionality Training**

The Site Review Meeting is scheduled to determine Client satisfaction and acceptance:

- Board books, book archives, calendar, contacts and resource center are reviewed for completeness and layout.  
Determination that the Diligent Service performs in accordance with this Exhibit A and the Documentation.
- Board books will be produced in accordance with the Specifications set forth herein and the Documentation.

## **IMPLEMENTATION PLAN – cont'd**

### **PHASE 2 (week 6-8)**

#### Board Presentation

Prior to the commencement of the roll-out to the board, upon request, Diligent attends a board meeting, and provides a 15-30-minute initial introduction and training for board members.

#### Director Training

	<p>Following the presentation to the board, and in coordination with the administrative team, Diligent arranges a one-on-one web training session with each board member. During this training, the User's log-in credentials are handed over to the User, and it is confirmed that the User can log-in, change their password and access the materials.</p> <p><u>First Paperless Meeting</u></p> <p>Once the board has been trained, then Client is ready to execute the first paperless meeting, and receive the full benefits of the Diligent Service implementation.</p> <p><u>Meeting Follow Up</u></p> <p>Following the first paperless meeting, the Diligent account management team will schedule a meeting to review how the meeting went, and identify any desired changes to the workflow and training or IT issues that need to be resolved ahead of the next meeting.</p> <p><u>6-month Review Meeting</u></p> <p>Customer Success Team and the Client will review the service, solution and transition from the conventional method used prior to introduction of the Diligent Service. The purpose of the meeting will be to discover any unresolved issues, address any other potential user cases and to update the Client on future product developments.</p>
--	--

<b>Offboarding</b>	<p>The offboarding plan for this Call-Off Contract is as follows:  After termination of this Agreement, Diligent will notify Client of the deletion date for Client Data on Diligent production systems. Within sixty (60) days of such deletion date, any backups of Client Data shall be deleted. During the Term, Client will be able to download a copy of Client Data.</p>
<b>Collaboration agreement</b>	Not used

<b>Limit on Parties' liability</b>	<p>Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed the annual Call-Off Contract value 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>£1,000</b> or 100% 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>£1,000</b> or 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<b>Insurance</b>	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>• professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim 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>
<b>Buyer's responsibilities</b>	<p>The Buyer is responsible for ensuring staff are available for training sessions and provision of a room for training unless training takes place via an online video meeting platform.</p>
<b>Buyer's equipment</b>	N/A

## Supplier's Information

<b>Subcontractors or partners</b>	The following is a list of the Supplier's Subcontractors or Partners Available at <a href="https://www.diligent.com/gdpr-subscription/">https://www.diligent.com/gdpr-subscription/</a>
-----------------------------------	--

## Call-Off Contract Charges and Payment

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

<b>Payment method</b>	The payment method for this Call-Off Contract is by BACS.
<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 NHS Business Services Authority and contact information nhsbsa.accountspayable@nhs.net.
<b>Invoice information required</b>	Not Used.
<b>Invoice frequency</b>	Invoice will be sent to the Buyer annually.
<b>Call-Off Contract value</b>	The total value of this Call-Off Contract is <b>GBP 28,000.00</b> (the initial value) The total maximum contract value, including the Extension Period and up to 50% optional growth, is GBP 63,000.00.

Call-Off Contract charges	The breakdown of the Charges is: PRICING AND FEES				
	<b>Description</b>	<b>Detail</b>	<b>Qty</b>	<b>Annual Price Per</b>	<b>Total Annual Price</b>
	Diligent Boards Standard Package	Diligent Boards Standard Package	1	████	████
	Sites	Sites	1	████	████
	Administrators	Administrators	5	████	████
	Users (Board Members/Executives)	Users (Board Members/Executives)	23	████	████
	Committees/Meeting Groups - No Charge	Committees/Meeting Groups - No Charge	10	████	████
	<b>TOTAL ANNUAL SUBSCRIPTION FEE</b>				████
	<b>ONE TIME INSTALLATION FEE</b> (set-up, installation and training for above configuration)		0	████	████

Additional Buyer Terms

<b>Performance of the Service</b>	<ul style="list-style-type: none"> <li>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones outlined above, subject at all times to the Buyer providing reasonable support to enable Supplier to meet such obligations and execution of this Call-Off Contract.</li> </ul>
<b>Guarantee</b>	Not used.
<b>Warranties, representations</b>	Not used.
<b>Supplemental requirements in addition to the Call-Off terms</b>	Not used.
<b>Alternative clauses</b>	Not used.
<b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b>	Not used.

<b>Personal Data and Data Subjects</b>	Schedule 7 is being used
<b>Intellectual Property</b>	The Buyer does not acquire any intellectual property or other rights, express or implied, in or relating to any Software or Diligent Services
<b>Social Value</b>	.Diligent ESG is a cloud based, purpose-built ESG and Sustainability software solution. At it's core, Diligent ESG provides elegant solutions data capture, validation and reporting, global emissions calculations and conversion. Additional modules, such as Report Authoring, enable sustainability reporting, global emissions calculations and conversions. Additional modules enable sustainability report curation, supplier surveys, and ESG investor questionnaire response composition, all on a single, secure, easy to use global platform.

## 1. Formation of Contract

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

## 2. Background to the agreement

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

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

<b>Signed</b>	Supplier	Buyer
<b>Name</b>	[Enter name]	[Enter name]
<b>Title</b>	[Enter title]	[Enter title]
<b>Signature</b>		
<b>Date</b>	[Enter date]	[Enter date]

## 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 invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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



- 11.8 Clause 11.6 will not apply if the IPR Claim is from:
- 11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.8.2 other material provided by the Buyer necessary for the Services
- 11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12 Protection of Information

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

## 13. Buyer data

- 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
- 13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

- 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
- 13.6.1 the principles in the Security Policy Framework: <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy: <https://www.gov.uk/government/publications/government-securityclassifications>
  - 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
  - 13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>
  - 12.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: <https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>
  - 13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
  - 13.6.6 Buyer requirements in respect of AI ethical standards.
- 13.7 The Buyer will specify any security requirements for this project in the Order Form.
- 13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## 14. Standards and Quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:  
  
<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15. Open Source

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

## 16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
  - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was

under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:  
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

## 17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

## 18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

- 18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- 18.4.2 any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- 18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- 18.5.2 an Insolvency Event of the other Party happens
- 18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

## 19. Consequences of Suspension, Ending and Expiry

- 19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.
- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- 19.4.1 any rights, remedies or obligations accrued before its Ending or expiration
- 19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry
- 19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
- 7 (Payment, VAT and Call-Off Contract charges)
  - 8 (Recovery of sums due and right of set-off)
  - 9 (Insurance)
  - 10 (Confidentiality)
  - 11 (Intellectual property rights)

- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
- 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

19.5.4 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

19.5.5 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

19.5.6 work with the Buyer on any ongoing work

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

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

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

## 20. Notices

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

- Manner of delivery: 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 Supplier 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

## 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 If the Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy an 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.

### 31.1 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

## Diligent Boards Overview

The Diligent Service known as Diligent Boards provides an internet-based portal that enables Client to manage its board and other materials through a site dedicated to Client Data (Client's "**Diligent Boards Site**"). Client's Diligent Boards Site is a secured location in the Diligent Service which is designed to be accessed only by authorized Users with a unique User ID and password. The Client's administrative staff prepares the board materials, which are then uploaded through the Diligent OneClick application. Those materials are then converted by the Diligent Service so that they can be accessed and viewed by Users electronically, in a format that can be accessed through the Client Software or a standard web browser. Available access rights are set forth in Sections 1, 2 and 3 below, and the Order reflects Client's chosen access rights. For clarity, Content Services are separate from Diligent Boards and are not within scope of this Exhibit.

### 1. Assigned Groups

**Site:** A Diligent Boards Site for a number of Users of the Diligent Service with access to a set of uploaded materials.

**Committee:** A meeting group within the Site that permits more limited access to certain materials for a particular group of Users.

### 2. User Types

**Users (Board Members/Executives):** Users with the ability to view the Client's documents using a supported web browser or Client Software

**Administrators:** Users with the ability to upload, collate, print, view, approve and publish Client's Board and Committee documents.

### 2. Additional Capabilities

**D&O Questionnaires Module:** This module provides seamless questionnaire integration.

**Messenger:** This module adds messaging functionality for Users through the Diligent Messenger Client Software.

**Evaluations Questionnaires Module:** This module provides survey capability for the purpose of board evaluations, and automated reporting and analysis of the data gathered from the surveys.

**Minutes Module:** This module enables Client to enhance minute taking with a tool that is integrated with Diligent Boards and enables Client to take minutes and assign action items.

Diligent Nominations: This Content Service is separate from but supplements the Diligent Boards service offering by providing proprietary governance analytics and information about companies and individuals.

For the avoidance of doubt, only those access rights listed in the Order are included in the pricing selected under this Agreement. For the avoidance of doubt, future additional access rights offering new functionality may be made available at additional cost. A Diligent representative can provide pricing for access rights not listed in the Order.

#### **4. Access for Administrators**

The Diligent Service allows all designated Administrators, i.e., the company secretary and administrative personnel, to upload, collate, print, view, approve and publish the Client's board and committee documents.

Configuration of this feature includes:

Set-up and customization of the Client's Diligent Boards Site for use by Administrators, including:

Project planning meeting, including review of current work flow and identification of key milestones, leading to development of an implementation plan that fits Client's needs and priorities

Collection of User survey information, mapping board and committee membership

Creation of a dedicated Diligent Boards Site

Creation and configuration of User accounts

Configuration of password policy and security configuration

Installation of Diligent OneClick

Configuration and installation of off-line features on the Administrator's laptop computer

#### **5. Online and Offline Access for Users**

While online, Users can view the Client's documents using a supported web browser or the Client Software. Each User can access the Diligent Boards Site with a User ID through the Client Software and supported web browsers.

Offline functionality allows Users to download materials from the Client's Diligent Boards Site via the internet and view them using the Client Software when the internet is not accessible. Configuration of this feature includes the capability to securely download and store an encrypted version of Client's materials to a designated laptop or supported mobile device and view materials when not connected to the internet.

#### **6. Implementation Process**

After execution of this Agreement, Diligent will assign an account management team to work with and train Client's Users in accessing and using the Diligent Service. The goal is to work directly with Client to streamline the process of preparing, approving and delivering board materials to deliver a system that the Users (regardless of their technological expertise) will quickly, easily and enthusiastically embrace and use. A sample implementation plan is included at the end of this Exhibit.

Diligent's one-on-one approach to the implementation process for the Diligent Service includes:

- Review of the present board preparation, workflow, and approval processes
- A technical profile of each User

- Recommended implementation strategy for Users based on their individual level of technological expertise and Client's objectives
- Ongoing general consulting regarding board material preparation and distribution

## **7. Training and Support**

Diligent training for Users includes:

- Separate training session(s) for the Administrators. Training includes instruction on log-in procedures, password usage, creating and building a Diligent Service file/database, editing and making changes, and uploading/converting files into the Diligent Service format for easy viewing by Users
- A separate training session for Users who wish to become familiar with the Diligent Service technology prior to the first board meeting
- One-on-one web training sessions with Users
- Ongoing training, including training for new Users, on-site or via web-conferencing, on an as-needed basis
- User guides for quick, easy reference.

Diligent's "Concierge" level of support reflects its understanding of the importance of being available 24/7/365 to assist every User and provide them with the comfort of knowing that Diligent is listening and responding to their needs, concerns and requirements.

- All Users have 24/7/365 personal assistance, via a toll-free number, to receive any help they need as well as answers to any Diligent application-related questions, at no additional cost.

Remote diagnostics and troubleshooting (including network and firewall issues) is provided for each User anywhere, anytime, as needed, at no additional cost.

## **8. Updates**

Updates to the Diligent Service and Client Software are included at no additional cost.

## **9. Failover/ Backup**

The Diligent Service includes a fault tolerant system configuration that is included at no additional cost. Client Data will reside on the Client's Diligent Boards Site in a primary data center, which is replicated to a secondary data center every four hours. Each data center is capable of delivering the Diligent Service. Additionally, each data center is built with hardware and network redundancy to offer continuous delivery of the Diligent Service. System availability is continuously monitored and failover is initiated if a primary data center becomes unavailable.

## **10. Security**

Diligent uses encryption algorithms, consistent with generally-accepted standards and practices adopted and implemented by software-as-a-service ("SAAS") providers, designed to limit unauthorized access to Client Data. Each User will have a unique User ID and password which will be required for the User to access Client's Diligent Boards Site. Diligent enforces password strength requirements, including frequency of password changes, according to Client's request.

Diligent uses a layered approach to security architecture, making use of firewalls, intrusion prevention systems, reverse web proxies, and segregation of specific application functions to provide security and integrity of the overall environment.

Upon request, more detailed information on Diligent's extensive security measures and protocols can be provided. Technical questions may be addressed to the appropriate salesperson or account management teams, who will engage the appropriate persons from Diligent's network, security and operational departments.

Clients may also elect to turn on two factor capability/device authorization for Users. These features offer enhanced security for Users accessing the Diligent Service by requiring additional verification of a User's identity (beyond User ID and password). This can be by means of a separate two factor token or via the User's device itself. For the avoidance of doubt, two factor tokens are available solely for the PC for an additional fee, while Device Authorization, offering authentication for the iPad and other supported devices, is available at no additional cost.

## **11. Client Requirements**

In order to use the Diligent Service, Client and Users must satisfy Diligent's minimum technology requirements, which, as of the Effective Date, are available at [www.diligent.com/tech-specs](http://www.diligent.com/tech-specs). The URL where such requirements are stored may change, but a current version of Diligent's minimum technology requirements is available from Diligent at any point upon request. All subscription costs for wireless and WiFi services must be covered by the Client / User.

## **12. Documentation**

Diligent will provide Client with access to Documentation relating to the Diligent Service and Client Software. Documentation and Specifications may be delivered using electronic means. Client may make a reasonable number of copies of the documentation to train and support its Users in their use of the Diligent Service and Client Software; however, Client must retain all copyright and proprietary notices on each copy of the Documentation made by Client.



## 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:

### PRICING AND FEES

Description	Detail	Qty	Annual Price Per	Total Annual Price
Diligent Boards Standard Package	Diligent Boards Standard Package	1	██████	██████
Sites	Sites	1	██████	██████
Administrators	Administrators	5	██████	██████
Users (Board Members/Executives)	Users (Board Members/Executives)	23	██████	██████
Committees/Meeting Groups - No Charge	Committees/Meeting Groups - No Charge	10	██████	██████
<b>TOTAL ANNUAL SUBSCRIPTION FEE</b>				██████
<b>ONE TIME INSTALLATION FEE</b> (set-up, installation and training for above configuration)		0	██████	██████

## Schedule 3: Collaboration Agreement

Not used.

## Schedule 4: Alternative Clauses

Not used.

## Schedule 5: Guarantee

Not used.

## Schedule 6: Glossary and Interpretations

In this Call-Off Contract the following expressions mean:

<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>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.

**Default**

Default is any:

- breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)
- other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract

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.

**DPA 2018**

Data Protection Act 2018.

**Employment Regulations**

The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .

**End**

Means to terminate; and Ended and Ending are construed accordingly.

**Environmental Information Regulations or EIR**

The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.

**Equipment**

The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

**ESI Reference Number**

The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.

**Employment Status Indicator test tool or ESI tool**

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:

<https://www.gov.uk/guidance/check-employment-status-fortax>

**Expiry Date**

The expiry date of this Call-Off Contract in the Order Form.

**Force Majeure**

A force Majeure event means anything affecting either Party's performance of their obligations arising from any:

- acts, events or omissions beyond the reasonable control of the affected Party
- riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare
- acts of government, local government or Regulatory Bodies
- fire, flood or disaster and any failure or shortage of power or fuel

- industrial dispute affecting a third party for which a substitute third party isn't reasonably available

The following do not constitute a Force Majeure event:

- any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain
- any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure
- the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans

**Former Supplier**

A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).

**Framework Agreement**

The clauses of framework agreement RM1557.13 together with the Framework Schedules.

**Fraud**

Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.

**Freedom of Information Act or FoIA**

The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.

**G-Cloud Services**

The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.

**UK GDPR**

The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).

**Good Industry Practice**

Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

**Guarantee**

The guarantee described in Schedule 5.



<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative Test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information Security Management System</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency event</b>	<p>Can be:</p> <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> </ul>
<b>Intellectual Property Rights or IPR</b>	<p>a Dun &amp; Bradstreet rating of 10 or less</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> </ul> <p>applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction all other rights having equivalent or similar effect in any country or jurisdiction</p>
<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul>
<b>IPR claim</b>	<p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). As set out in clause 11.5.</p>

<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 Outside IR35</b>	G-Cloud Services which are the subject of an order by the Buyer.  Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the UK GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the UK GDPR.
<b>Platform</b>	The government marketplace where Services are available for Buyers to buy.
<b>Processing</b>	Takes the meaning given in the UK GDPR.
<b>Processor</b>	Takes the meaning given in the UK GDPR.
<b>Prohibited Act</b>	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and

	services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's highperformance 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</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Security Management Plan</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Services</b>	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.
<b>Service Definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Platform.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls">https://www.gov.uk/service-manual/agile-delivery/spend-controls</a> <u>ck-if-you-need-approval-to-spend-money-on-a-service</u>

<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 GCloud 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

For the purposes of this Schedule, the Buyer shall be the “Client” and the Supplier shall be the “Supplier”.

The Parties enter into this Addendum with respect to Personal Data regulated under Data Protection Law and (1) that is provided to Supplier by or on behalf of Client and which is Processed by Supplier as Processor, (2) that is shared between the Parties on a Controller to Controller basis, (3) that Client will make available to Supplier and which is regulated by the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations (“**CCPA**”), or (4) that is subject to the GDPR, Swiss law or United Kingdom law and is transferred, directly or via onward transfer, to a Party who is located outside any member state of the European Economic Area (“**EEA**”), Switzerland, or the United Kingdom.

Capitalized terms used in this Addendum shall have the meaning given to them in Section 5 (Definitions), unless otherwise specified.

The terms in this Addendum shall be incorporated into and form part of the Call Off Contract between Client and Supplier governing Client’s use of Supplier’s software-as-a-service and online services (including professional services or related components delivered by Supplier) (“**Agreement**”), and the Agreement and this Addendum shall be read as one document. In the event of conflict with any other terms of the Agreement, this Addendum shall prevail. For the avoidance of doubt, this Addendum need not be separately executed by the Parties if this Addendum is already explicitly incorporated into a fully executed Agreement, in which event the Parties’ signature to such Agreement shall be deemed signature to this Addendum.

In the event that Data Protection Laws are amended, replaced or repealed, the Parties shall where necessary negotiate in good faith a solution to enable the transfer of Personal Data to be conducted in compliance with Data Protection Laws.

### 1. CONTROLLER TO PROCESSOR RELATIONSHIP

A. Client shall act as Controller and Supplier shall act as a Processor when Processing any Personal Data contained within Client Data or Service Data provided to Supplier by Client for the purposes of (a) providing the software-as-a-service subscription purchased by Client under the Agreement, and/or any other services Supplier provides under the Agreement, or (b) otherwise performing Supplier’s obligations under the Agreement (the “**Services**”). In these circumstances, Supplier shall:

- (1) process the Personal Data on behalf of Client only in accordance with the Agreement, this Addendum, Client’s written instructions, and Data Protection Laws; and
- (2) not collect, retain, use, disclose, or sell the Personal Data for any purpose. For the avoidance of doubt, Client instructs Supplier to Process the Personal Data as reasonably necessary and proportionate to achieve Client’s and Supplier’s business purposes to the extent permitted by Data Protection Laws

Details of this Processing are set out in Schedule 1 attached to this Addendum

B. Supplier agrees that it will, to the extent required by applicable Data Protection Laws when acting as a Processor in the provision of the Services:

- (1) process the Personal Data only for the purpose of providing the Services or as otherwise instructed in writing by Client. If Supplier is legally required to process Personal Data otherwise than as instructed by Client, it will notify Client before such processing occurs, unless the law requiring such processing prohibits Supplier from notifying Client;
- (2) inform Client if any instruction contradicts any legal requirements to which Supplier is subject;
- (3) keep all Personal Data confidential as required under the Agreement and ensure that persons authorised by Supplier to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (4) provide access to Personal Data only to those of its employees, Affiliates or Subprocessors who need access to such data for the purposes set out in Section 1.A;
- (5) take appropriate technical and organizational security measures designed to safeguard Personal Data against unauthorized access, destruction, disclosure, transfer, or other improper use as set forth in Schedule 2 attached to this Addendum;
- (6) provide Client with access to the Personal Data which have been provided by Client to enable Client to comply with its obligations to Data Subjects exercising their rights under Data Protection Laws. Supplier shall refer such Data Subjects to Client and shall also, at the request of Client, use its reasonable endeavors to either (a) amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects to ensure that their Personal Data are accurate and complete or (b) provide the Client with the ability to directly amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects through the Services;
- (7) promptly notify Client of any accidental or unauthorized access, destruction, disclosure, transfer of Personal Data that have been supplied by Client, after Supplier becomes aware of any such access, destruction, disclosure, transfer or other improper use, or of any complaints by individuals or third parties that involve or pertain to such Personal Data, and shall, taking into account the nature of the Processing and the information available to Supplier, provide such assistance to Client as may be reasonable in the circumstances to enable Client meet its obligations to notify any Supervisory Authority or any other regulatory or governmental authorities or Data Subjects of such event where Client is required to do so by law;
- (8) taking into account the nature of the Processing and the information available to Supplier, use reasonable endeavors to assist Client (a) in complying with Client's obligation to implement appropriate technical and organizational security measures; and (b) in relation to any privacy impact assessments or consultations with Supervisory Authorities about the Processing of Personal Data in the context of the provision of the Services or any inquiry, complaint or claim in relation to the Processing by Supplier of Personal Data provided by Client;

- (9) make available to Client all information necessary to demonstrate that Supplier is in compliance with Data Protection Laws;
- (10) allow Client to audit Supplier by receiving reasonably reliable documentation regarding the adequacy of the Processing by the Supplier of Personal Data on behalf of the Client. Such documentation may: (a) be an annual SOC2 (or subsequent successor) audit of the Supplier's security policies and procedures; (b) be in accordance with ISO 27001 standards or such alternative standards that are substantially equivalent to ISO 27001; or (c) otherwise provide for demonstrable assurances of adequacy of the data processing facilities used by the Supplier to Process Personal Data on behalf of the Client, including penetration tests or vulnerability scans ("Audit Report"). If the Client requests in writing, Supplier will provide the Client with a copy of the Audit Report or related documentation so that the Client can reasonably verify the Supplier's compliance with the security obligations under Data Protection Laws. Unless otherwise required by a Supervisory Authority or mutually agreed by the Parties in writing, any audit of Supplier shall be limited to the provision of the Audit Report;
- (11) at the termination of the Agreement or this Addendum, at Client's election, delete or return the Personal Data to Client, provided that Client acknowledges and agrees that any Personal Data stored within the software-as-a-service offerings provided by Supplier to Client shall be deleted either as specified within the Agreement or, if the Agreement is silent, within thirty (30) days of termination of the Agreement; and
- (12) the Client acknowledges and agrees that Supplier may retain Affiliates and other third parties as Subprocessors in connection with this Agreement, having imposed on such Subprocessors substantially similar data protection obligations as are imposed on Supplier under this Agreement. Supplier shall remain liable to the Client for the act and omissions of the Subprocessors under this Agreement as if they were Supplier's own acts and omissions. Any updates to Subprocessors are available at <https://diligent.com/gdpr-subscription> or a successor website as made available by Supplier for this purpose and notified to Client (the "Subprocessor Site"). Client may be informed of new Subprocessors by visiting the Subprocessor Site or by subscribing for Subprocessor updates using the process outlined on the Subprocessor Site. In the event Supplier adds or replaces a Subprocessor, Client may object to the use of a new Subprocessor by sending a notification to [privacy@diligent.com](mailto:privacy@diligent.com) within ten (10) business days of receipt of notice of a new Subprocessor provided that the Client reasonably believes that use of such Subprocessor presents an unreasonable risk to or prevents the Client from complying with applicable law. If Client so objects, Supplier shall either (a) not use the new Subprocessor to process the Client Personal Data or (b) shall find an alternative way of reasonably resolving Client's objection. If neither (a) nor (b) is reasonably feasible within thirty (30) days of receipt of Client's objection, then Client shall either rescind its objection or may terminate any services for which the new Subprocessor would be used by providing written notice to Supplier at the address for notices indicated in the Agreement. For the avoidance of doubt, in the event Client does not object to a new Subprocessor in accordance with this Section, Client shall be deemed to have consented to the new Subprocessor.



- C. To the extent that the provision of the Services under this Section 1 involves the transfer of Personal Data that is subject to the GDPR, Swiss law, or United Kingdom law by Client (as Data Exporter) to Supplier (as Data Importer) outside the EEA, Switzerland, or the United Kingdom (either directly or via onward transfer), and Supplier is not located in a country which has been recognised by the relevant Supervisory Authority as offering an adequate level of protection for Personal Data transferred to it, the Parties agree to either (a) comply with the terms of Module 2 of the Transfer Clauses (where Client acts as a Controller) or Module 3 of the Transfer Clauses (where Client acts as a Processor retaining Supplier as an additional Processor), which Transfer Clauses are incorporated herein by reference; or (b) otherwise Process such Personal Data using a valid transfer mechanism in accordance with Data Protection Laws.
- D. Where the Supplier, acting as a Processor (and as Data Exporter), transfers Personal Data that is subject to the GDPR, Swiss law, or United Kingdom law to the Client acting as a Controller (and as Data Importer), and the Client is located and/or Processes the Personal Data in a country which is not considered under an adequacy decision of the relevant Supervisory Authority to provide for a level of data protection as considered adequate pursuant to applicable Data Protection Laws, the Parties shall transfer such Personal Data in accordance with the Transfer Clauses (Module 4), which are incorporated herein by reference, and Data Protection Laws.

## **2. CONTROLLER RELATIONSHIPS**

- A. Section 1 above does not apply where Supplier is acting as a Controller. Supplier may make available certain Services that enable the Client to access Content. To the extent that Client Processes any Personal Data contained within such Content, the relationships of the Parties shall be that of independent Controllers with respect to such Personal Data (and not joint controllers as defined under the GDPR) and each Party shall comply with its respective obligations under the Data Protection Laws and any applicable privacy policy
- B. To the extent that Client Processes any Personal Data contained within such Content, Client agrees and warrants that it will:
- (1) process Personal Data contained within the Content for the purposes of its obligations under this Addendum or Agreement and in accordance with Data Protection Laws;
  - (2) not share any Personal Data contained within the Content with any third party without Supplier's prior consent or authorization;
  - (3) ensure that any Personal Data contained within the Content is processed fairly, lawfully, and in a transparent manner;
  - (4) provide reasonable cooperation and assistance to Supplier, upon Supplier's request, in relation to Personal Data contained within the Content, including complaints or requests from Data Subjects to exercise their rights, or any request, instruction, complaint, investigation or audit by any Supervisory Authority;
  - (5) notify Supplier without undue delay upon becoming aware of any Personal Data Breach affecting any Personal Data contained within the Content and

taking reasonable action to minimize the impact of such event and prevent such event recurring; and

- (6) implement and maintain appropriate and technical and organizational measures to protect any Personal Data within the Content against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.
- C. To the extent that Supplier Processes Personal Data provided to it by Client for purposes other than as set forth in Section 1.A above, Supplier acknowledges that it will be a Controller of that Personal Data, and Supplier agrees to Process such Personal Data in accordance with Data Protection Laws.
- D. Where the Supplier, acting as a Controller (and as Data Exporter), transfers Personal Data that is subject to the GDPR, Swiss law, or United Kingdom law to the Client (as Data Importer) in accordance with Section 2.A, and the Client is located and/or Processes the Personal Data in a country outside the EEA, Switzerland, or the United Kingdom which is not considered under an adequacy decision of the relevant Supervisory Authority to provide for a level of data protection as considered by that Supervisory Authority to be adequate pursuant to applicable Data Protection Laws, the Parties shall transfer such Personal Data in accordance with the Transfer Clauses (Module 1), which are incorporated herein by reference, and Data Protection Laws.

### **3. CLIENT OBLIGATIONS**

- A. In relation to all Personal Data provided by Client to Supplier for Processing under the Agreement, Client shall ensure that:
  - (1) where consent is required for Vendor's Processing under applicable Data Protection Laws, all relevant Data Subjects have consented (in accordance with applicable Data Protection Laws) to their Personal Data being disclosed to Vendor for Processing in accordance with the Agreement;
  - (2) the disclosure of Personal Data by Client to Vendor will be in each case and in all respects lawful;
  - (3) notice of the disclosure of their Personal Data to Vendor for Processing in accordance with the Agreement and this Addendum will be provided to all relevant Data Subjects (including any Users) prior to any such disclosure and, if requested by Vendor, Client shall provide evidence that it has provided such notice;
  - (4) Client complies with, and represents and warrants that it has complied with, applicable Data Protection Laws in relation to the disclosure of such Personal Data to Vendor, its use of the Services and the performance of the Agreement by Client and its Users;
  - (5) it shall not, by any act or omission, put Vendor or any of its Affiliates or subsidiaries in breach of any Data Protection Laws; and
  - (6) it shall do and execute, or arrange to be done and executed, each act, document and thing necessary or desirable in order to comply with this Section 3.

### **4. TRANSFER CLAUSES**

A. Where the Transfer Clauses apply under this Addendum:

- (1) Client and Supplier agree to observe the terms of the Transfer Clauses without modification and the Transfer Clauses shall be considered to be duly executed by the Parties immediately upon the date on which this Addendum enters into force;
- (2) the rights and obligations afforded by the Transfer Clauses will be exercised in accordance with the terms of this Addendum; in case of any conflict between the terms of the Transfer Clauses and any other part of this Addendum or the Agreement, the Transfer Clauses shall prevail;
- (3) the Parties elect to add the optional Clause 7 (Docking Clause) of the Transfer Clauses and do not elect to add the additional optional language under Clause 11(a) (Redress) of the Transfer Clauses;
- (4) for purposes of Clause 17 (Governing Law) of the Transfer Clauses, the Parties elect Option 1, and the Parties agree that this shall be the law of Ireland;
- (5) for purposes of Clause 18 (Choice of Forum and Jurisdiction) of the Transfer Clauses, the Parties agree that any dispute arising from these Clauses shall be resolved by the courts of an EU Member State. The Parties agree that those shall be the courts of Ireland.
- (6) the Parties' signature to this Addendum or an Agreement that explicitly incorporates this Addendum shall be considered as signature to the Transfer Clauses;
- (7) if so required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Transfer Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required; and
- (8) in the event that the Transfer Clauses are amended, replaced or otherwise invalidated by the European Commission or under the Data Protection Laws, the Parties shall work together in good faith to enter into any updated version of such Transfer Clauses or negotiate in good faith a solution to enable a transfer of the Personal Data to meet the requirements of Chapter V of the GDPR.

B. In addition, with respect to Module 2 and/or Module 3 of the Transfer Clauses, the following additional provisions shall apply:

- (1) the Parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Transfer Clauses shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's written request;
- (2) the Parties agree that the audits described in Clause 8.9 of the Transfer Clauses shall be carried out in accordance with Section 1.B(9) and (10) of this Addendum; and
- (3) for purposes of Clause 9(a) of the Transfer Clauses, the Parties elect Option 2 (General Written Authorisation), it being understood that Client provides the general authorisation and instruction for the engagement of the Subprocessors

from the agreed list of Subprocessors available on the Subprocessor Site, and the Parties agree to observe the provisions set out in clause 1.B(12) of this Addendum in relation to any additions or replacements of Subprocessors on such list; for purposes of Clause 9(a) of Module 3 of the Transfer Clauses, where Client acts as Processor, the Client (1) warrants that it has the authority to provide such general authorisation and instruction on behalf of the Controller, and (2) agrees to inform the Controller of any addition or replacement of Subprocessors on the agreed list for and on behalf of Vendor (thereby enabling the Vendor to comply with its obligation under Clause 9(a) of the Transfer Clauses);

- (4) for purposes of Clause 8.6(c) and (d) (Security of Processing) of Module 3 of the Transfer Clauses, where Client acts as Processor, the Parties acknowledge and agree that it will not be appropriate and feasible for Vendor to directly notify the Controller of a Personal Data Breach concerning Personal Data Processed by Vendor under the Transfer Clauses, and Client agrees to forward to the Controller any such notification of a Personal Data Breach without undue delay;
- (5) for purposes of Clause 8.9 (Documentation and Compliance) of Module 3 of the Transfer Clauses, where Client acts as Processor, Client agrees that all inquiries from the Controller shall be provided to Vendor by the Client (for and on behalf of the Controller) and, except as determined necessary by Vendor to ensure that inquiries are promptly and adequately be dealt with, all relevant communication shall be handled solely via the Client. In case Vendor receives an inquiry directly from the Controller, it shall promptly forward the inquiry to the Client;
- (6) for purposes of Clause 10 of Module 3 (Data Subject Rights) of the Transfer Clauses, where Client acts as Processor, the Parties acknowledge and agree that it will not be appropriate for Vendor to directly notify the Controller of any request it has received from a Data Subject, and Client agrees to promptly forward to the Controller any such notification and to be primarily responsible to assist the Controller in fulfilling the relevant obligations to respond to any such request, it being understood that Vendor will provide assistance and cooperation to Client in accordance with this Addendum;
- (7) for the avoidance of doubt, Vendor's relationships with Subprocessors may still be governed by previous iterations of the Transfer Clauses as of the date of this Addendum, and this shall not be treated as a breach of this Addendum or the Agreement until such time as such previous iterations are no longer recognized as having legal impact under GDPR;
- (8) for purposes of Clause 13 of the Transfer Clauses, the competent supervisory authority shall be the supervisory authority identified by Client on the signature page of this Addendum or, if Client does not so identify a competent supervisory authority on the signature page of this Addendum, the competent supervisory authority shall be the supervisory authority of the Member State in which the data exporter is established or has appointed a representative pursuant to Article 27(1) of the GDPR, and such competent supervisory authority shall be incorporated into Annex I.C of the Transfer Clauses; and
- (9) Schedules 1 and 2 of this Addendum shall serve as Annexes I and II respectively of the Transfer Clauses.

- C. In addition, with respect to Module 1 of the Transfer Clauses, the following additional provisions shall apply:
- (1) Schedule 3 of this Addendum shall serve as Annex I of the Transfer Clauses.
- D. In addition, with respect to Module 4 of the Transfer Clauses, the following additional provisions shall apply:
- (1) Schedule 4 of this Addendum shall serve as Annex I of the Transfer Clauses.
- E. In addition, with respect to Modules 1, 2, 3, and 4 of the Transfer Clauses, where transfers of Personal Data are subject to United Kingdom law, the Transfer Clauses shall be amended and subject to the following additional provisions:
- (1) Part 2: Mandatory Clauses of 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 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses ("Approved Addendum");
  - (2) The information required by Part 1 of the Approved Addendum is set out at Schedule 1-4 of this Addendum (as applicable);
  - (3) With respect to Section 19 of the Approved Addendum, in the event the Approved Addendum changes, neither party may end the Addendum except as provided for in the Approved Addendum or the Agreement; and
  - (4) Any references to the "Clauses" in the Transfer Clauses shall include the amendments set out in this Section 4.E(5).
- F. In addition, with respect to Modules 1, 2, 3, and 4 of the Transfer Clauses, where transfers of Personal Data are subject to Swiss law, the Transfer Clauses shall be amended and subject to the following additional provisions:
- (1) the term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with the Transfer Clauses;
  - (2) the Transfer Clauses also protect the data of legal entities until the entry into force of the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023 ("Revised FADP"); and
  - (3) the FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

## 5. DEFINITIONS

- A. For the purposes of this Addendum:
- (1) "**Affiliate**" means, with respect to any legally recognizable entity, any other entity Controlling, Controlled by, or under common Control with such entity. "Control" means direct or indirect (i) ownership of more than fifty percent (50%) of the outstanding shares representing the right to vote for members of the board of directors or other managing officers of such entity, or (ii) for an entity that

does not have outstanding shares, more than fifty percent (50%) of the ownership interest representing the right to make decisions for such entity. An entity will be deemed an Affiliate only so long as Control exists.

- (2) **"Client Data"** means all data successfully uploaded, entered, created and stored by the Client within the Diligent software-as-a-service offerings for which Client has a subscription;
- (3) **"Content"** means any data, data structure, metadata, metrics, charts, graphs, literature, or other content in any form and/or any derivatives thereof that are made available by Vendor within any of its Services, including, where applicable, all updates delivered thereto (but at all times excluding Client Data);
- (4) the terms **"Controller"**, **"Personal Data Breach"**, **"Processor"**, **"Process(ing)"**, and **"Data Subject"**, with respect to Personal Data subject to the GDPR, each have the meaning given to such terms in the GDPR, and with respect to all other Personal Data, "Controller" means the entity responsible for deciding the purpose and means for Processing Personal Data and "Processor" means the entity that Processes Personal Data on behalf of the Controller. Any references to Vendor as a "Processor" shall include, as applicable, Vendor as a "service provider" as that term is defined in the CCPA;
- (5) the terms **"Data Exporter"** and **"Data Importer"** have the meaning given to them in the Transfer Clauses;
- (6) the term **"Data Protection Laws"** means any applicable laws, regulations, or other binding obligations (including any and all legislative and/or regulatory amendments or successors thereto), each as updated from time to time, of the European Union, the EEA, Switzerland, the United Kingdom, the United States, or any other jurisdiction that govern or otherwise apply to Personal Data Processed under the Agreement, including the GDPR and the CCPA;
- (7) the term **"Diligent Group Entity"** shall mean Diligent Corporation and/or each of its Affiliates which has signed this Addendum or an Agreement that explicitly incorporates this Addendum;
- (8) the term **"GDPR"** shall mean European Union Regulation 2016/679 and includes any relevant implementing measure in each relevant Member State, or any successor legislation thereto;
- (9) **"Personal Data"** means any information that relates to, identifies, describes, is capable of being associated with, or could reasonably be linked to, directly or indirectly, an identified or identifiable individual, or to the extent applicable under Data Protection Laws, an identified or identifiable household;
- (10) **"Service Data"** means any Personal Data of Users which is required to provide the Services, such as User ID, User type, name, company affiliation, contact information (business address, phone number, and email address) as well as any Personal Data Processed to perform specifically contracted professional services;
- (11) **"Services"** shall have the meaning described in Section 1.A;

- (12) "**Subprocessor**" means a Processor appointed by Vendor to assist with the provision of the Services to the Client or the performance of Vendor's obligations under the Agreement;
- (13) the term "**Supervisory Authority**" shall mean the data protection authority in the applicable Member State of the European Union and the equivalent authorities in each other state within the EEA, Switzerland, the United Kingdom or any other jurisdiction whose Data Protection Laws apply to the Processing of the Personal Data subject to this Addendum;
- (14) the term "**Transfer Clauses**" shall mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
- (15) "**User**" means any individual authorized to make use of the Services pursuant to the Agreement; and
- (16) Any capitalized terms not defined in this Section 5 shall be defined as they are under the Agreement.

## 2. GOVERNING LAW AND MISCELLANEOUS

The Parties will enter into all such additional agreements or terms as may be necessary to ensure the lawful Processing of Personal Data for the purposes of Data Protection Laws and the Agreement and to ensure the receipt of all necessary approvals for such Processing from appropriate regulatory authorities where applicable, and will co-operate with each other as reasonably necessary in order to obtain such approvals or execute such additional agreements or terms as soon as reasonably possible. Except with respect to the Transfer Clauses, this Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed in all respects by, and construed in accordance with, the governing law of the Agreement.

Except as otherwise stated herein, this Addendum shall supersede and replace all previous provisions of the Agreement related to Data Protection Laws. Any pre-existing audit rights are superseded by Section 1.B(9) and (10) of this Addendum.

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

# **Annex 1: Processing Personal Data**

## **EXHIBIT I – Module 2 and Module 3**

This Schedule forms part of the Addendum and also serves as Annex I to Module 2 and/or Module 3 of the Transfer Clauses.

### **A. List of Parties**

#### **Data Exporter**

**Name:** the Client entity as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Address:** as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Contact person's name, position and contact details:** as identified on this signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Activities relevant to the data transferred under Module 2 and/or 3 of the Transfer Clauses:**

**Client shall be** providing Personal Data as necessary to receive the Services pursuant to the Agreement and this Addendum, and as Supplier is further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws and Regulations, to achieve Supplier's business purposes.

**Role: Controller or Processor (as appropriate)**

#### **Data Importer**

**Name:** the Supplier entity (or entities) as defined under this Addendum.

**Address:** as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Contact person's name, position and contact details:** John Van Arsdale, Data Protection Officer of the Diligent group of companies, [privacy@diligent.com](mailto:privacy@diligent.com)

**Activities relevant to the data transferred under Module 2 of the Transfer Clauses:**

**With respect to Module 2 of the Transfer Clauses, Supplier shall** Process Personal Data as necessary to perform the Services pursuant to the Agreement and this Addendum, and as further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws and Regulations, to achieve Supplier's business purposes.

**Role: Processor**



## **Description of the Processing and Transfer**

### **Categories of Data Subjects whose personal data is processed and may be transferred**

Client may submit Personal Data to the Supplier, the extent of which is determined and controlled by the Client in its discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Client's customers, business partners, Suppliers, and other third parties of Client, employees, directors, officers, contact persons, and Users authorized to use the Supplier services.

### **Categories of personal data processed and which may be transferred**

The Client may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by the Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data: Name; home address; photograph; professional email address; professional telephone number (including mobile telephone number); personal email address; personal telephone number (including mobile telephone number); data related to transactions including transactions' purposes; tax ID; government identification number; inclusion on a government issued list or watchlist; customer numbers; complaints; bank account details; marketing preferences; IP address; cookie data; login credentials (username and password); traffic data including web logs; images.

### **Special categories of data/Sensitive data processed and which may be transferred (if applicable)**

The Client may, subject to any restrictions set forth in the Agreement, submit special categories of data to the Supplier, the extent of which is determined and controlled by the Client in its sole discretion, and which is for the sake of clarity is Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation. In any event, any such Personal Data may only be submitted as Client Data. Supplier personnel shall avoid accessing any such Personal Data except where Client specifically elects to provide such Personal Data to Supplier

### **Frequency of the Transfer**

The Personal Data will be transferred on a continuous basis for as long as Client has a valid subscription to the relevant Services, unless otherwise specifically agreed elsewhere between Client and Supplier.

### **Nature of the Processing**

Supplier will Process Personal Data as necessary to perform the Services pursuant to the Agreement and this Addendum on behalf of the Client, and as further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws, to achieve Supplier's business purposes.

### **Purpose(s) of the Data Transfer and Processing**

The purpose of the data transfer and processing is to fulfil the objectives of the Agreement between Supplier and Client, in particular delivery of the Services as contemplated under the Agreement and this Addendum.

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

For the Duration as set forth below and as otherwise agreed upon by the Parties or specifically required by applicable law.

### **Subject Matter of the Processing**

The subject matter of the Processing is enabling the Client to receive the value of the Services as contemplated under this Addendum and the Agreement, including enabling the Supplier to deliver support, customer success, and the Services, including enabling the security of Services. For the avoidance of doubt, if the Client elects to host Client Data outside the EEA, Switzerland or the United Kingdom, the Transfer Clauses shall apply to such transfer.

### **Duration**

The Personal Data will be Processed by Supplier for the duration of the Services.

### **Competent Supervisory Authority**

The competent supervisory authority in accordance with Clause 13 of the Transfer Clauses shall be the EU supervisory authority as identified on the signature page to this Addendum and/or as specified by Section 4.B.(8) of the Addendum.

## EXHIBIT 2

### Technical and Organisational Measures

This Schedule forms part of the Addendum and serves as Annex II to the Transfer Clauses

**Description of the technical and organisational measures implemented and maintained by the Supplier (or document/legislation attached):**

Supplier will maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data, including those measures specified in the Agreement. Supplier's relevant security Documentation as applicable to the Services, including audit reports and/or security test reports where applicable, is available upon request.

Supplier provide Client with access to the Personal Data which have been provided by Client to enable Client to comply with its obligations to Data Subjects exercising their rights under Data Protection Laws. Supplier shall refer such Data Subjects to Client and shall also, at the request of Client, use its reasonable endeavors to either (a) amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects to ensure that their Personal Data are accurate and complete or (b) provide the Client with the ability to directly amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects through the Services;

## EXHIBIT 3 – Module 1

This Schedule serves as Annex I to Module 1 of the Transfer Clauses where applicable

### A. List of Parties

#### Data Exporter

**Name:** the Supplier entity (or entities) as defined under this Addendum

**Address:** as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Contact person's name, position and contact details:** John Van Arsdale, Data Protection Officer of the Diligent group of companies, [privacy@diligent.com](mailto:privacy@diligent.com)

#### Activities relevant to the data transferred under Module 1 of the Transfer Clauses:

With respect to Module 1 of the Transfer Clauses, Supplier shall provide Personal Data as necessary to perform the Services pursuant to the Agreement and this Addendum where such Services include the delivery of Content to the Client.

**Role: Controller**

### B. Description of the Transfer

#### Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of Data Subjects:

- corporate directors, officers, and employees, as well as others whose activities in each case are a matter of public interest in relation to corporate governance, risk management, and compliance.

#### Categories of personal data transferred

The personal data transferred concern personal data which may include (without limitation):

- name; job title and level; date of birth; employer; departments; work location; age; gender; remuneration; shareholdings; corporate directorships and tenure; nationality; education (qualification/degree, major, honors, duration); sectoral experience; disciplinary history; peer associations; appearances in publications; photograph.

#### Special categories of data/Sensitive data transferred (if applicable)

None anticipated.

#### Frequency of the Transfer

The Personal Data will be transferred on a continuous basis for as long as Client has a valid subscription to the relevant Services, unless otherwise specifically agreed elsewhere between Client and Supplier.

## **Nature of the Processing**

**Personal Data shall be transferred to Client by Supplier in the course of Client receiving certain Content as part of the Services where Client has subscribed to such Services.**

## **Purpose(s) of the Data Transfer and Further Processing**

The transfer is made for the following purposes:

- to provide certain subscription services involving the delivery of Content that may contain personal data of public interest, including reference data and benchmarking related to corporate governance, compensation, and company well-being, as well as curated news content, to Client.

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

For the term of the subscription to the relevant Services and as otherwise agreed upon by the Parties or specifically required by applicable law. Each of Supplier and Client shall be required to follow its own data retention policies, which shall at all times comply with the requirements of applicable law.

3.

## **C. Competent Supervisory Authority**

The competent supervisory authority in accordance with Clause 13 of the Transfer Clauses shall be the Data Protection Commissioner of Ireland.

## EXHIBIT 4 – Module 4

This Schedule serves as Annex I to Module 4 of the Transfer Clauses where applicable:

### A. List of Parties

#### Data Exporter

**Name:** the Supplier entity (or entities) as defined under this Addendum.

**Address:** as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Contact person's name, position and contact details:** John Van Arsdale, Data Protection Officer of the Diligent group of companies, [privacy@diligent.com](mailto:privacy@diligent.com)

**Activities relevant to the data transferred under Module 4 of the Transfer Clauses:**

With respect to Module 4 of the Transfer Clauses, Supplier shall Process Personal Data as necessary to perform the Services pursuant to the Agreement and this Addendum, and as further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws and Regulations, to achieve Supplier's business purposes.

**Role:** Processor

#### Data Importer

**Name:** the Client entity as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Address:** as identified on the signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Contact person's name, position and contact details:** as identified on this signature page to this Addendum or in the Agreement that explicitly incorporates this Addendum.

**Activities relevant to the data transferred under Module 4 of the Transfer Clauses:**

Client shall provide and subsequently receive Personal Data from the Supplier in the course of receiving Services pursuant to the Agreement and this Addendum where such Services involves the Processing Personal Data by the Processor.

**Role:** Controller

### B. Description of the Transfer

#### Categories of Data Subjects whose personal data is transferred

Client may submit Personal Data to the Supplier, the extent of which is determined and controlled by the Client in its discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Client's customers, business partners, Suppliers, and other third parties of Client, employees, directors, officers, contact persons, and Users authorized to use the Supplier services.

## **Categories of personal data transferred**

The Client may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by the Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data: Name; home address; photograph; professional email address; professional telephone number (including mobile telephone number); personal email address; personal telephone number (including mobile telephone number); data related to transactions including transactions' purposes; tax ID; government identification number; inclusion on a government issued list or watchlist; customer numbers; complaints; bank account details; marketing preferences; IP address; cookie data; login credentials (username and password); traffic data including web logs; images.

## **Special categories of data/Sensitive data transferred (if applicable)**

The Client may, subject to any restrictions set forth in the Agreement, submit special categories of data to the Supplier, the extent of which is determined and controlled by the Client in its sole discretion, and which is for the sake of clarity is Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or sex life or sexual orientation. In any event, any such Personal Data may only be submitted as Client Data. Supplier personnel shall avoid accessing any such Personal Data except where Client specifically elects to provide such Personal Data to Supplier.

## **Frequency of the Transfer**

The Personal Data will be transferred on a continuous basis for as long as Client has a valid subscription to the relevant Services, unless otherwise specifically agreed elsewhere between Client and Supplier.

## **Nature of the Processing**

Supplier will Process Personal Data as necessary to perform the Services pursuant to the Agreement and this Addendum on behalf of the Client, and as further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws, to achieve Supplier's business purposes.

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

For the term of the subscription to the relevant Services and as otherwise agreed upon by the Parties or specifically required by applicable law. Each of Supplier and Client shall be required to follow its own data retention policies, which shall at all times comply with the requirements of applicable law.

## **Subject Matter of the Processing**

The subject matter of the Processing is enabling the Client to receive the value of the Services as contemplated under this Addendum and the Agreement, including enabling the Supplier to deliver support, customer success, and the Services, including enabling the security of Services.

**Duration**

The Personal Data will be Processed by Supplier for the duration of the Services



