

# Framework Schedule 6 (Order Form Template and Call-Off Schedules)

## Order Form

CALL-OFF REFERENCE: **WP2155 GOV.UK Site Search Product**

THE BUYER: **Cabinet Office (Government Digital Service)**

BUYER ADDRESS: **Cabinet Office:** Cabinet Office, 1 Horse Guards Road, London, SW1A 2HQ.  
**Government Digital Service:** The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

THE SUPPLIER: **Google Cloud EMEA Limited**

SUPPLIER ADDRESS: 70 Sir John Rogerson's Quay, Dublin 2, D02  
R296 Republic of Ireland

REGISTRATION NUMBER: **660412**

DUNS NUMBER: **985760329**

SID4GOV ID: **N/A**

### APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 1 November 2023, which will be implemented from a Supplier-selected date that is no later than 5 business days after the Call-off Contract Start Date (the "**Implementation Date**").

It's issued under the Framework Contract with the reference number RM6195 for the provision of Big Data & Analytics.

CALL-OFF LOT(S):  
**Lot 2**

### **CALL-OFF INCORPORATED TERMS**

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:



1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6195
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
  - Joint Schedules for RM6195
    - o Joint Schedule 2 (Variation Form)
    - o Joint Schedule 3 (Insurance Requirements)
    - o Joint Schedule 4 (Commercially Sensitive Information)
    - o Joint Schedule 10 (Rectification Plan)
    - o Joint Schedule 11 (Processing Data)
  - Call-Off Schedules for **WP2155**
    - o Call-Off Schedule 1 (Transparency Reports)
    - o Call-Off Schedule 5 (Pricing Details)
    - o Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - o Call-Off Schedule 9 (Security)
    - o Call-Off Schedule 15 (Call-Off Contract Management)
    - o Call-Off Schedule 20 (Call-Off Specification)
  - CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6195
6. [Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.]

Save for Appendix 1 (Call-Off Special Terms), no other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

**CALL-OFF SPECIAL TERMS**  
**Set out in Appendix 1 below.**

CALL-OFF START DATE:	<b>1 November 2023</b>
CALL-OFF EXPIRY DATE:	<b>31 October 2025</b>
CALL-OFF INITIAL PERIOD:	<b>2 x 12 months</b>
CALL-OFF OPTIONAL : EXTENSION PERIOD:	<b>2 periods of up to 12 months each. Subject to Cabinet Office Approvals</b>

**The Buyer can extend the contract for 2 periods of up to 12 months each - subject to Cabinet Office approvals.**

## **CALL-OFF DELIVERABLES**

GOV.UK [site search](#) is one of the key ways that users find information on GOV.UK. Millions of search queries are made each month to help users find vital information on GOV.UK.

GOV.UK site search is currently powered by a self-hosted database.

GOV.UK is now seeking to procure a software as a service search solution to improve GOV.UK site search.

Our goals with site search are:

- to significantly improve the quality of the GOV.UK site search experience for users by improving the relevancy of results
- to reduce the long term maintenance work required of the GOV.UK team.

These Deliverables are further detailed in Call-Off Schedule 20 (Specification).

## **Technical Requirements**

The following requirements are must-have requirements for the search product, as further detailed in Call-Off Schedule 20 (Specification).

		Requirement
1	Data	The product provides indexing, search and retrieval of over 550k documents with an average indexed document size of 25Kb each
2	Data	The product provides an indexing API or endpoint for published documents to be pushed for indexing
3	Data	The product supports English (en_GB) language content
4	Data	The product supports up to 240 different metadata attributes/fields per document with different data types, searching, retrieval, filtering, faceting requirements per attribute
5	Querying	The product provides querying in English (en_GB) language
6	Querying	The product provides querying for exact phrase matches
7	Querying	The product provides querying for exact identifiers in appropriate attributes
8	Querying	The product provides querying for known entities in data

<b>9</b>	Querying	The product provides querying on selected attributes/fields from the data
<b>10</b>	Querying	The product provides retrieval of selected attributes/fields from the data
<b>11</b>	Querying	The product provides provides appropriate spelling suggestions based on data against misspellings
<b>12</b>	Querying	The product provides term close variants in searches
<b>13</b>	Relevance	The product provides querying and discovery of data using Keyword search principles
<b>14</b>	Relevance	The product provides querying and discovery using Natural Language and Keywords
<b>15</b>	Relevance	The product provides querying and discovery of data using Semantic/Vector search principles
<b>16</b>	Relevance	The product utilises Large Language Models for query understanding
<b>17</b>	Relevance	The product provides querying and discovery of data using Generative AI
<b>18</b>	Relevance	The product provides relevancy quality assessment through judgement lists
<b>19</b>	Relevance	The product provides hybrid querying and discovery through a combination of search principles
<b>20</b>	Relevance	The product provides relevancy influence through document popularity signals
<b>21</b>	Relevance	The product provides relevancy influence through document recency signals
<b>22</b>	Filtering and Faceting	The product provides filtering on documents with specified values in defined attributes
<b>23</b>	Filtering and Faceting	The product provides generation of facets/aggregations for defined attributes based on search scope
<b>24</b>	Filtering and Faceting	The product provides generation of document counts for attribute values in facets/aggregations
<b>25</b>	Filtering and Faceting	The product provides change of filter scope on individual attribute facets/aggregations

<b>26</b>	Filtering and Faceting	The product provides rejection of documents without specified values in defined attributes
<b>27</b>	Filtering and Faceting	The product provides filtering on documents missing specified attributes
<b>28</b>	Filtering and Faceting	The product provides ordering of facet values by document count, value or whether they are being filtered on
<b>29</b>	Sorting	The product provides sorting of search results by relevance
<b>30</b>	Sorting	The product provides sorting of search results by newest date
<b>31</b>	Sorting	The product provides sorting of search results by other defined text / date attributes
<b>32</b>	Retrieval	The product provides retrieval individual document records by identifier
<b>33</b>	Retrieval	The product provides total count of relevant documents in search results
<b>34</b>	Retrieval	The product provides the highlighting of relevant terms within records in search response
<b>35</b>	Rules	The product provides mechanisms to boost/bury specific documents under specific query conditions
<b>36</b>	Rules	The product provides mechanisms for rules to be managed programatically
<b>37</b>	Rules	The product provides custom synonyms for known domain specific synonyms
<b>38</b>	Rules	The product provides expedient removal of rules from results
<b>39</b>	Client integration	The product provides REST API querying interface
<b>40</b>	Client integration	The product provides integration libraries for Ruby integration
<b>41</b>	Workflow	The product provides infrastructure as code
<b>42</b>	Workflow	The product supports the provisioning of up to 3 environments for Production, Staging and Integration
<b>43</b>	Workflow	The product provides mechanisms (e.g. aliases/branches) to allow data and model changes to be introduced without service disruption

<b>44</b>	Indexing	The product provides high volume indexing throughput - up to 2k records per batch
<b>45</b>	Indexing	The product provides low latency indexing throughput - records must be available in search results within 5 minutes of publishing
<b>46</b>	Indexing	The product provides the expedient removal of selected data records in emergency circumstances
<b>47</b>	Operations	The product provides serverless architecture
<b>48</b>	Operations	The product provides integration with external operational observability platforms and patterns
<b>49</b>	Performance	The product provides low query response times (0.4 seconds or under)
<b>50</b>	Performance	The product provides high volume query requests per second (50 per second)
<b>51</b>	Reliability	The product provides high availability (99.9%) and failover to maintain query service
<b>52</b>	Reliability	The product provides dynamic scaling to maintain querying performance during traffic spikes
<b>53</b>	Disaster recovery	The product provides the support backup/restore of data for recovery in the case of service disruption

### **Product Requirements**

The search product must demonstrate the use of the latest search technology, to generate relevant results and have the following characteristics

1. The product is simple for developers to integrate and configure
2. The product supports querying and discovery of data using semantic search
3. The product supports the querying and discovery of data using generative AI
4. The product supports relevancy by using a range of different signals

### **Security Requirements**

Supplier's compliance with the requirements in this section will be further detailed in the Security Management Plan.

All GOV.UK data must be stored and processed on systems hosted in the UK or EU, data centres hosting data outside of these areas will not be acceptable and will be in breach of GDS Security policies unless an International Data Transfer Agreement (IDTA) to process data outside the UK or EU is in place and can be provided, as

further detailed in GDS Supplier Security Schedule, Annex 1 - Security Management Schedule (Supplier-led Assurance) and Section 6 (GDS Security Schedule - Data Location Requirements) of the Call-Off Special Terms (Appendix 1).

To safeguard the GOV.UK data and identify any vulnerabilities in the proposed hosting centre, regular annual penetration testing is required as a minimum annually.

Vendors must have relevant user authentication and security and authentication systems in place such as SSO and MFA.

The Supplier must follow where applicable:

- The Government Technology Code of Practice  
<https://www.gov.uk/guidance/the-technology-code-of-practice>
  - The Government Service Standard and Service Manual  
<https://www.gov.uk/service-manual/service-standard>
  - NCSC Cyber Assessment Framework Guidance  
<https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework>
  - NCSC guidance  
<https://www.ncsc.gov.uk/section/advice-guidance/all-topics>
  - Government Functional Security Standard No.7  
<https://www.gov.uk/government/publications/government-functional-standard-govs-007-security>
  - NCSC Cloud Security Principles;  
<https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>
  - Cyber Essentials plus certification
  - ISO 27001 and; or SOC2
  - ISO 27701
  - The Supplier to evidence their resources are BPSS clearance level or equivalent demonstrated.
1. Subject to Section 1.1 below, the Supplier will ensure compliance with GDS Supplier Security Schedule, Security Management Schedule (Supplier-led Assurance) ("**GDS Security Schedule**").
- 1.1 The parties acknowledge and agree that the Supplier's compliance with (i) the Standards applicable to this Call-Off Contract set out in Section 6 (Standards) of Schedule 1 (Specification) of the Framework Agreement and (ii) the requirements in the GDS Security Schedule will be agreed between the parties and documented in the Security

Management Plan in accordance Section 2 below, taking into account the nature of the Services provided under this Call-Off Contract and any equivalent security standards and practises the Supplier currently has in place.

2. The Supplier must provide a Security Management Plan (SMP) within 20 days of contract agreement, Annex 2 Security Management Plan.
3. The Supplier must engage in Security Working Groups as required by the Buyer.  
Frequency;
  - First SWG following receipt of the SMP
  - Thereafter quarterly as agreed at SWG.
4. The Supplier will engage in performance management reviews as required by the Buyer. Frequency; Initial session; monthly with agreed timelines thereafter.

### **Support Requirement**

The Vendor must provide as a minimum the following support requirements  
24/7 incident response - 1 hour initial response time for P1 incidents and 4 hour response time for P2 incidents, which will be provided as part of the Enhanced Support TSS.

### **MAXIMUM LIABILITY**

The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £274,500.00 (excluding VAT).

### **CALL-OFF CHARGES**

The value of the contract is **\$356,854 USD (approximately £274,500.00)** per annum and a total of **\$713,707 USD (approximately £549,000.00)** for the 24 months (excluding taxes) from 1 November 2023 until 31 October 2025. The maximum value of spend for that period is anticipated by GDS to be **\$1,560.000 USD (approximately £1,200,000.00)** (excluding taxes) and is subject to the details provided in Call-Off Contract Schedule 5 (Pricing Details).

If the contract is extended beyond 31 October 2025 for a maximum of 12 months (1 November 2025 - 31 October 2026), the contract value could increase to **\$2,340,000 USD (approximately £1,800,000.00)** (excluding taxes) maximum. This is subject to Cabinet Office approvals.

If the contract is extended beyond 31 October 2026 for a maximum of 12 months (1 November 2026 - 1 November 2027), the contract value could increase to

**\$3,120,000 USD (approximately £2,400,000.00)** (excluding taxes) maximum. This is subject to Cabinet Office approvals.

**Please see Breakdown of the cost in Call-Off Schedule 5 - Pricing Details.**

[REDACTED]

**REIMBURSABLE EXPENSES**

Not applicable.

**PAYMENT METHOD**

The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.

PO Number to be issued by the Buyer following execution of this Call-Off Contract.

**BUYER'S INVOICE ADDRESS:**

Invoices will be sent to:

[REDACTED] and [REDACTED]

which is at Cabinet Office, PO Box 405, SSCL, Phoenix House, Celtic Springs Business Park, Newport, NP10 8FZ.

**BUYER'S AUTHORISED REPRESENTATIVE**

**Name:** [REDACTED]

**Role:** [REDACTED]

**Email address:** [REDACTED]

**Address:** Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

**Name:** [REDACTED]

**Role:** [REDACTED]

**Email address:** [REDACTED]

**Address:** Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

**Name:** [REDACTED]

**Role:** [REDACTED]

**Email address:** [REDACTED]

**Address:** Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

Name: [REDACTED]

Role: [REDACTED]

Email address: [REDACTED]

Address: Government Digital Service: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS

### **BUYER'S ENVIRONMENTAL POLICY**

Cabinet Office Environment policy, available at request. Please email GDS Commissioning Team ([commissioning-digital@digital.cabinet-office.gov.uk](mailto:commissioning-digital@digital.cabinet-office.gov.uk) / [GDS-digital-buyer@digital.cabinet-office.gov.uk](mailto:GDS-digital-buyer@digital.cabinet-office.gov.uk))

### **BUYER'S SECURITY POLICY**

Cabinet Office Security Breach Policy, Physical Security Policy and Personnel Vetting Policy, all available on request. Please email GDS Commissioning Team ([commissioning-digital@digital.cabinet-office.gov.uk](mailto:commissioning-digital@digital.cabinet-office.gov.uk) / [GDS-digital-buyer@digital.cabinet-office.gov.uk](mailto:GDS-digital-buyer@digital.cabinet-office.gov.uk)).

Supplier's compliance with Cabinet Office (GDS Supplier Security Schedule) and Security Terms in the Order Form will be agreed between the parties following signature of the CoC and documented in the Security Management Plan.

### **SUPPLIER'S AUTHORISED REPRESENTATIVE**

Name: [REDACTED]

Email Address: [REDACTED]

Address: Belgrave House, 76 Buckingham Palace Road, Victoria, LONDON, SW1W 9TQ

### **SUPPLIER'S CONTRACT MANAGER**

Name: [REDACTED]

Role: [REDACTED]

Email Address: [REDACTED]

Address: Belgrave House, 76 Buckingham Palace Road, Victoria, LONDON, SW1W 9TQ

### **PROGRESS REPORT FREQUENCY**

Progress Report to be provided on a monthly. Please refer to Order Schedule 1 (Transparency Report).

### **PROGRESS MEETING FREQUENCY**

Progress meeting frequency should be conducted on monthly basis.

### **KEY STAFF**

Name: [REDACTED]

**Role:** [REDACTED]  
**Email Address:** [REDACTED]  
**Address:** Belgrave House, 76 Buckingham Palace Road, Victoria, LONDON, SW1W 9TQ

**Name:** [REDACTED]  
**Role:** [REDACTED]  
**Email Address:** [REDACTED]  
[REDACTED] Palace Road, Victoria, LONDON, SW1W 9TQ

**KEY SUBCONTRACTOR(S)**

Not Applicable

**COMMERCIALLY SENSITIVE INFORMATION**

Please see Commercially Sensitive document. Please refer to Joint Schedule 4 (Commercially Sensitive Information).

**SERVICE CREDITS**

Not Applicable

**ADDITIONAL INSURANCES**

Not Applicable

**GUARANTEE**

Not Applicable

**SOCIAL VALUE COMMITMENT**

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender).

For and on behalf of the Supplier: Google Cloud EMEA Limited		For and on behalf of the Buyer: Cabinet Office ( <i>Government Digital Service</i> )	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

## APPENDIX 1

### CALL-OFF SPECIAL TERMS

#### 1. Definitions

**“Audited Services”** means the then-current services indicated as being in-scope for the relevant certification or report at

<https://cloud.google.com/security/compliance/services-in-scope> Services will not be removed from this URL unless they have been discontinued in accordance with the Call-Off Contract.

**“Customer Application”** means a software program that Customer creates or hosts using the Services.

**“High Risk Activities”** means activities where the use or failure of the Services would reasonably be expected to lead to death, personal injury, or environmental or property damage (such as the creation or operation of nuclear facilities, air traffic control, life support systems, or weaponry).

**“Key Services”** means the then-current list of services at <https://cloud.Supplier.com/terms/key-services>. Supplier may not remove a service from this URL unless that service is discontinued in accordance with Section 5.1.2.

**“Project”** means a collection of Google Cloud Platform resources configured by Customer via the Services.

**“Security Whitepaper”** means the then-current security and compliance documentation that is available at <https://cloud.google.com/security/whitepaper>

**“Supplier API”** means any application programming interface provided by Supplier as part of the Services.

**“Supplier Order Form”** means the order form attached in Annex 1 of Appendix 1 (Call-Off Special Terms) in the Order Form.

**“Supplier Terms”** means the following terms:

- **“Acceptable Use Policy”** or **“AUP”** located at <https://cloud.Supplier.com/terms/aup> which applies to Buyer’s use (and its end users) of the Services;
- **“Cloud Data Processing Addendum”** or **“CDPA”** located at <https://cloud.google.com/terms/data-processing-addendum> which describes the parties’ obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer

Data (as defined therein) in addition to those set out in Joint Schedule 11 (Data Processing);

- “**Service Levels**” or “**SLAs**” located at <https://cloud.google.com/terms/sla> which describes each of the then-current service level agreements applicable to the Services;
- “**Service Specific Terms**” located at <https://cloud.google.com/terms/service-terms> which apply to one or multiple Services; and
- “**TSS Guidelines**” located at <https://cloud.google.com/terms/tssg> which describes Supplier’s technical support services guidelines.

## **2. Supplier Order Form**

- 2.1.** The Supplier Order Form included in Annex 1 to this Order Form amends the Call-off Contract under which the Supplier has agreed to provide the Services to the Buyer and is required to enable Buyer’s purchase of the Services in accordance with the Supplier’s standard processes.

## **3. Amendments to Core Terms**

- 3.1.** For the purposes of this Call-Off Contract only, the following Clauses of the Core Terms are amended as follows:
- 3.1.1. Clauses 7.1 to 7.4 (Supplier Staff) shall be deleted and replaced with “Not used”.
  - 3.1.2. Clause 14.3 (Back-ups of Government Data) shall be deleted and replaced with “Not used”.
  - 3.1.3. The notification timeframe of “immediately” in Clauses 14.5 (Government Data Loss/Degradation) and 15.1(c) Core Terms shall be replaced with “without undue delay”.
  - 3.1.4. Clause 15.3 (What you must keep confidential) shall be deleted and replaced with “Not used” .

## **4. Buyer obligations in respect of the Supplier Terms**

### **4.1. Acceptable Use Policy**

- 4.1.1. Compliance. Buyer will ensure that it and its Personnel and end users' use of the Services comply with the AUP.
- 4.1.2. Restrictions. Buyer will not, and will not allow its Personnel or end users to access or use the Services (i) for High Risk Activities or (ii) in violation of the AUP.
- 4.1.3. AUP Violations. If Supplier becomes aware that Buyer's or any of its Personnel or end user's use of the Services violates the AUP, Supplier will notify Buyer and request that Buyer correct the violation. If Buyer fails to correct the violation within 24 hours of Supplier’s request, then the Supplier may Suspend all or part

of Buyer's use of the Services until the violation is corrected.

**4.2. Cloud Data Processing Addendum**

- 4.2.1. General. The CDPA applies to Buyer's use of the Services. The Buyer confirms that the execution of this Call-Off Contract constitutes its written consent to the transfer of Customer Personal Data (as defined in the Supplier Terms) outside of the UK and EU in accordance with the Supplier Terms and the GDS Security Schedule and as required by Section 6(d) of Joint Schedule 11 (Processing Data).
- 4.2.2. Protection of Customer Data. The Supplier will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Supplier has implemented and will maintain technical, organizational, and physical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.
- 4.2.3. In the event of a Personal Data Breach pursuant to Section 7(f) of Joint Schedule 11 (Data Processing), the notification timeframe of "immediately" in shall be replaced with "without undue delay" in accordance with Section 7.2 (Data Incidents) of the Cloud Data Processing Addendum.

**4.3. Technical Support Services**

- 4.3.1. By Buyer. Customer is responsible for technical support of its Customer Applications and Projects.
- 4.3.2. By Supplier. Subject to payment of applicable support Charges, Supplier will provide TSS to the Buyer during the Call-Off Contract Period in accordance with the TSS Guidelines. Certain TSS levels include a minimum recurring fee as described at <https://cloud.Supplier.com/skus>. If Buyer downgrades its TSS level during any calendar month, Supplier may continue to provide TSS at the same level and for the same TSS Charges as applied before the downgrade for the remainder of that month.

**4.4. Service Levels**

- 4.4.1. The Supplier will provide the Services in accordance with the SLAs.

**5. Updates to Services and Terms**

**5.1. Changes to the Services**

- 5.1.1. Supplier may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.
- 5.1.2. Notwithstanding the above, Supplier may discontinue a Service (or associated material functionality), provided that Supplier will notify Buyer at least 36 months before discontinuing any Key Service (or associated material functionality), and at least 12 months before discontinuing any other Service (or associated material functionality), in each case unless Supplier replaces such discontinued Service or functionality with a materially similar Service or functionality.
- 5.1.3. Supplier will continue to provide product and security updates, and TSS, until the conclusion of the applicable notice period in Section 5.1.2 above.
- 5.1.4. Notwithstanding Section 5.1.1, Supplier may significantly modify a Buyer-facing Supplier API in a backwards-incompatible manner, provided that Supplier will notify Buyer at least 12 months before doing so.

**5.2. Changes to Terms**

- 5.2.1. Supplier may update the Supplier Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Supplier's processing of Customer Data as described in the Cloud Data Processing Addendum, or (c) have a material adverse impact on Buyer's rights under the Supplier Terms. Supplier will notify Buyer of any material changes to the Supplier Terms. Material changes to the Supplier Terms will be effective 30 days after Buyer receives notice of such changes.

**5.3. Permitted Changes**

- 5.3.1. Sections 5.1 (Changes to Services) and 5.2 (Changes to Terms) do not limit Supplier's ability to make changes required to comply with applicable Law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality. Notwithstanding Section 5.2 (Changes to Terms), material changes to the Supplier Terms made to comply with applicable Law or to address a material security risk will be effective upon notice.

**6. GDS Security Schedule - Data Location Requirements**

- 6.1. The parties agree that for the purposes of this Call-Off Contract, the Relevant Activities do not include undertaking Development Activities or hosting a Development Environment pursuant to paragraph 1.1(aa) and 1.1(bb) of Appendix 1 of the GDS Security Schedule.

- 6.2.** Subject to Sections 6.3 and 6.4 below, the Buyer acknowledges that it can configure its Services to meet its data location requirements detailed in paragraph 1 (Location) of Appendix 1 of the GDS Security Schedule pursuant to section 1 (Data Location) of the General Terms and section 14 (AI/ML Data Location) of the AI/ML Services terms in the Service Specific Terms and the Cloud Data Processing Addendum.
- 6.3.** Where the Supplier cannot meet the data location requirements detailed in paragraph 1.1 (Location for Relevant Activities) and paragraph 1.4 (Support Locations) of Appendix 1 of the GDS Security Schedule, the parties have agreed that, pursuant to paragraphs 1.2 and 1.5, the Supplier will carry out the Relevant Activities outside the UK/EEA. The Buyer acknowledges that the Supplier has provided the relevant information for such processing to evidence this in accordance with paragraphs 1.2(d) and 1.5(d) of Appendix 1 of the GDS Security Schedule.
- 6.4.** Vertex AI Search. For the purposes of section 14 (AI/ML Data Location) of the AI/ML Services in the Service Specific Terms, as at the date of this Call-Off Contract and subject to the “Vertex AI Search Locations” page at <https://cloud.google.com/generative-ai-app-builder/docs/locations#limitations>, the AI/ML Data Location commitment applies to Vertex AI Search as if it were listed at <https://cloud.Supplier.com/terms/data-residency> except that the activities listed in (a) and (b) therein will be performed in both EU and US Multi-Regions. This Section 6.4 applies unless and until Vertex AI Search is listed as at <https://cloud.Supplier.com/terms/data-residency>, at which point the Buyer may configure Vertex AI Search in its chosen Multi-Region.

## **7. Subcontractors**

- 7.1.** The Supplier confirms that as at the date of this Call-Off Contract, there are no Key Subcontractors in scope for the services provided under this Call-Off Contract.
- 7.2.** For the purposes of meeting the requirements in Clauses 10.8 (When subcontracts can be ended) and 23.6 (Transferring responsibilities - Subcontractor details) of the Core Terms, the following provisions will apply to Subcontractors (excluding Subprocessors):
- 7.2.1.** Buyer specifically pre-approves and authorises the engagement of the Subcontractors at the date of this Call-Off Contract. If Supplier engages a new Subcontractor or changes the function of an existing Subcontractor (a “**Subcontractor Change**”), Supplier will inform Buyer at least 180 days in advance, unless the Subcontractor Change is made to address an existing or imminent risk to the Services, in which case Supplier will provide

Buyer as much advance notice as is reasonably possible. If Buyer determines that a Subcontractor Change would materially increase Buyer's risk or Supplier does not inform Buyer of a Subcontractor Change as required in this Section, Buyer may terminate this Call-Off Contract for convenience. A list of the Supplier's Subcontractors used to deliver the Services, including their functions and locations, may be made available upon request from the Buyer.

## 8. Subprocessors

8.1. For the purposes of meeting the requirements in Section 13 (Consent to subprocessoring) of Joint Schedule 11 (Processing Data):

- 8.1.1. A list of the Supplier's Subprocessors, including their functions and locations, is available for Supplier Cloud Platform at: <https://cloud.Supplier.com/terms/subprocessors>. Buyer specifically authorises the engagement as Subprocessors of those entities listed at this URL as at the Call-Off Start Date. In addition, Buyer generally authorises the engagement as Subprocessors of any other third parties ("**New Subprocessors**").
- 8.1.2. When Supplier engages any New Subprocessor it will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Buyer of the engagement (including the name, location and activities of the New Subprocessor).
- 8.1.3. When any New Subprocessor is engaged during the Call-Off Contract Period, Supplier will, at least 30 days before the New Subprocessor starts processing any Customer Personal Data (as defined in the CDPA), notify Buyer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform). Buyer may, within 90 days after being notified of the engagement of a New Subprocessor, object by terminating this Call-Off Contract immediately by notifying Supplier. This termination right is Buyer's sole and exclusive remedy if Buyer objects to any New Subprocessor.
- 8.1.4. Further Supplier commitments with regards to Subprocessors are set out in Section 11 of the CDPA.

## 9. Deletion of Government Data / Personal Data

9.1. For the purposes of meeting the requirements in Clauses 10.6.1(d) Core Terms, Clauses 14.8(c) and (d) of the Core Terms and Section 6(e) of Joint Schedule 11 (Processing Data) regarding deletion of Government Data (including Personal Data), the Supplier will enable the Buyer to delete its own Government Data (including Personal Data) during the Call-Off Contract Period in a manner consistent with the

functionality of the Services, and the Buyer acknowledges that it is a Buyer responsibility to retrieve and delete the Government Data (including Personal Data) prior to termination or expiry of the Call-Off Contract in accordance with Section 6 (Data Deletion) of the CDPA.

## 10. Audit

10.1. The following additional terms will apply to any Audits carried out (including pursuant to Clauses 6.3 to 6.5 (inclusive) of the Core Terms):

### 10.1.1. Certifications and Audit Reports.

10.1.1.1. Independent Assessment. Supplier submits its systems and controls for the Services to industry-standard audits by a qualified and independent third party auditor (the “**Third Party Auditor**”). These audits validate Supplier’s adherence to defined controls and certifications based on the internationally accepted independent standards listed at <https://cloud.Supplier.com/security/compliance/services-in-scope>.

10.1.1.2. ISO Certifications and SOC Reports. Supplier will maintain at least the following for the Audited Services during the Term: (a) certificates for ISO 27001, ISO 27017 and ISO 27018, and its PCI DSS Attestation of Compliance (the “**Compliance Certifications**”); and (b) SOC 1, SOC 2 and SOC 3 reports produced by Supplier’s Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the “**SOC Reports**”). Supplier may add standards at any time. Supplier may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

10.1.1.3. Reviews of Security Documentation. Supplier will make the following available for review by Buyer during the Term: (a) the Compliance Certifications; (b) the SOC Reports; (c) the Security Whitepaper; and (d) any other documents relevant to the security or compliance of the Services that are made publicly available to customers of the Services (the “**Security Documentation**”).

10.1.1.4. Scope of Certifications and Audit Reports. To ensure that they remain an effective tool, if a key system or control for an Audited Service is not covered in the Compliance Certifications and SOC Reports (“**Certifications and Audit Reports**”), then:

- 10.1.1.4.1.** Modification requests. Buyer can request an expansion of the scope of the Certifications and Audit Reports for that Audited Service to such key systems and/or controls. Any request must be legitimate from a risk management perspective and based on then-current internationally accepted independent standards that are applicable to the Audited Service. Supplier will assess Buyer's request and may request further information from Buyer. If the expansion is already on Supplier's compliance roadmap, Supplier will confirm when it is currently scheduled to happen.
- 10.1.1.4.2.** Further assistance. Supplier will work with Buyer in good faith to consider alternative ways to assess the system or control using the existing Certifications and Audit Reports and/or the activities available to Buyer under Section 10.1.2 (Audit and Access).

**10.1.2. Audit and Access**

- 10.1.2.1.** If Section 10.1.1 above is deemed not sufficient by the Buyer for its Audit purposes, then, in accordance with the provisions of this Section, the Buyer may (a) review information about the Services and discuss it with Supplier Staff (including subject matter experts); and (b) audit and inspect the Services used by the Buyer and access Supplier's premises used to provide those Services to do so. To facilitate activities under this Section (Audit, and Access), Supplier and the Buyer will discuss scope and duration in advance. The Buyer may appoint any qualified and independent third party auditor to perform any activity under this Section ("**Buyer Auditor**"), provided that the Buyer Auditor is not a competitor of the Supplier.
- 10.1.2.2.** Audits will be conducted: (a) during business hours and, unless it is not possible due to an emergency or crisis situation or would lead to a situation where the activity would no longer be effective, at a time specified by Supplier or with reasonable notice; (b) in accordance with the Security Measures; and (c) in a way that minimizes disruption to Supplier's business and operations and Supplier's other customers' environments. Buyer is responsible for the acts and omissions of its Personnel

and end users and will ensure they comply with this  
Section.

# Google Cloud Platform



Customer	Quote ID	Date
----------	----------	------

10/30/2023

## Customer Details

GOV.UK Ops (GDS Business Operations)  
The White Chapel Building, 10 Whitechapel High  
St  
LONDON, E18QS  
United Kingdom

### Customer Billing Details

The White Chapel Building, 10 Whitechapel High St  
LONDON, E18QS  
United Kingdom

**Google Customer ID**

Sales Rep

Andrea Brewer

**Tax Exempt:**

**Google Reference No.**

VAT/GST/Tax Number (if appl.)

N/A

### Billing Account Administrator Details

(Contact will become the initial billing account administrator who can manage other user roles on the billing account in the Admin Console.)

Category	Item	Value	Unit
A	1	10	kg
	2	20	kg
	3	30	kg
	4	40	kg
	5	50	kg
	6	60	kg
	7	70	kg
	8	80	kg
B	1	10	kg
	2	20	kg
	3	30	kg
	4	40	kg
	5	50	kg
	6	60	kg
	7	70	kg
	8	80	kg
C	1	10	kg
	2	20	kg
	3	30	kg
	4	40	kg
	5	50	kg
	6	60	kg
	7	70	kg
	8	80	kg

[illegible]

PO # (if required)

Google Google Cloud EMEA Ltd

**Customer Government Digital Services, Cabinet Office**

Signature \_\_\_\_\_  
 Print Name \_\_\_\_\_  
 Title \_\_\_\_\_  
 Date \_\_\_\_\_

Signature \_\_\_\_\_  
 Print Name \_\_\_\_\_  
 Title \_\_\_\_\_  
 Date \_\_\_\_\_