Order Form

CALL-OFF REFERENCE:	Covid Inquiry Support Z2202141/Department for Business, Energy and Industrial Strategy/prj_403
THE BUYER:	Department for Business, Energy and Industrial Strategy
BUYER ADDRESS	1 Victoria Street, London, SW1H 0ET
THE SUPPLIER:	TLT LLP
SUPPLIER ADDRESS:	20 Gresham Street, London EC2V 7JE
REGISTRATION NUMBER:	OC308658
DUNS NUMBER:	739281603
SID4GOV ID:	N/A

It is essential that if you, as the Buyer, add to or amend any aspect of any Call-Off Schedule, then **you must send the updated Schedule** with the Order Form to the Supplier]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 20 July 2022.
It's issued under the Framework Contract with the reference number Legal Services Panel RM6179 for the provision of legal advice and services.

CALL-OFF LOT:
Lot 1 – General Legal Advice and Services

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) RM6179
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
   - Joint Schedules for RM6179
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)
     - Joint Schedule 4 (Commercially Sensitive Information)
     - Joint Schedule 10 (Rectification Plan)
     - Joint Schedule 11 (Processing Data)
   - Call-Off Schedules for **prj_403**
     - Call-Off Schedule 1 (Transparency Reports) (as set out below)
     - Call-Off Schedule 2 (Staff Transfer) (Part C and Part E only)
     - Call-Off Schedule 3 (Continuous Improvement) (managed at framework level)
     - Call-Off Schedule 7 (Key Supplier Staff)
     - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
     - Call-Off Schedule 9 (Security) (Part A may be required – see specification)
     - Call-Off Schedule 19 (Scottish Law)
     - Call-Off Schedule 20 (Call-Off Specification)
     - Call-Off Schedule 21 (Northern Ireland Law)
     - Call-Off Schedule 26 Non Disclosure Agreement template
     - Call-Off Schedule 25 (Secondment Agreement Template)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6179

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
The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1

The Supplier has numerous clients that rely upon it for general representation. The Supplier advises clients in matters arising under the laws of: one or more of the constituent parts of the United Kingdom, the European Union, a Member State of the European Union, the WTO, other international trade and/or investment agreements, or public international law

generally. As a result, without advance conflicts waivers from Supplier clients, conflicts of interest could arise that could deprive either the Buyer or other Supplier clients of the right to select the Supplier as counsel.

In light of the foregoing, other current or future clients of the Supplier including those identified in the preceding paragraph (collectively, the "Other Clients") may ask the Supplier to represent them in matters (including litigation) that are adverse to the Buyer but that are not substantially related to the Supplier's representation of the Buyer. If the Supplier is not representing the Buyer in such a matter, and the matter in which the Buyer and the Other Client have adverse interests is not substantially related to our current or past representation of the Buyer, then:

1. the Buyer agrees that the Supplier may represent such Other Client to the extent and provided that the Supplier is and remains not substantially related to the Supplier's representation of the Buyer;

2. the Buyer waives any conflict of interest arising from such representation; and

3. the Buyer agrees that it will not seek to disqualify or otherwise prevent the Supplier from representing such Other Client,

provided that any Confidential Information and Personal Data held by lawyers of the Supplier that assisted the Buyer in this matter is kept confidential, in the case of Confidential Information, and Processed, in the case of Personal Data, in accordance with Clauses 14 and 15 of the Core Terms, respectively.

The Buyer acknowledges that it has had an opportunity to consult with other counsel (in-house or otherwise) before agreeing to this waiver.

Special Term 2

See Annex 1 to this order form

CALL-OFF START DATE: 20 July 2022

CALL-OFF EXPIRY DATE: 31 March 2025
[OR On completion of the Deliverables]

CALL-OFF INITIAL PERIOD: 2 years, 8 months

CALL-OFF INITIAL PERIOD VALLUE: £6,000,000

[CALL-OFF OPTIONAL EXTENSION PERIOD: Until 30/11/2026

WORKING DAY
Any day other than a Saturday or Sunday or public holiday in England and Wales unless otherwise requested by the Buyer and agreed in advance.

CALL-OFF DELIVERABLES
The Buyer is entitled to 2 hours of free initial consultation and legal advice with each Order in accordance with Paragraph 5.2 of Framework Schedule 1 (Specification).

See details in Call-Off Schedule 20 (Call-Off Specification)

MANAGEMENT OF CONFLICT OF INTEREST
In the event that a conflict arises through the course of the provision of the Services which the Buyer agrees in writing that the conflict can be managed to their satisfaction, Call Off Special Term 1 will apply, and any particular arrangements or mitigating steps shall be agreed in writing with the Buyers Authorised Representative.

CONFIDENTIALITY
See Call Off Schedule 26 (Non Disclosure Agreement template)

IPR
N/A

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, and as amended by the Framework Special Terms.

CALL-OFF CHARGES
Hourly Rates

Fee Earner	**Hourly Price**
Partner	[redacted]
Legal Director	[redacted]
Senior Solicitor	[redacted]
Solicitor	[redacted]
Junior Solicitor	[redacted]
Trainee / Paralegal	[redacted]
Legal Project Manager	[redacted]

The Charges will not be impacted by any change to the Framework Prices.

VOLUME DISCOUNTS
Where the Supplier provides Volume Discounts, the applicable percentage discount (set out in Table 2 of Annex 1 of Framework Schedule 3 (Framework Prices)) shall automatically be applied by the Supplier to all Charges it invoices regarding the Deliverables on and from the date and time when the applicable Volume Discount

threshold is met and in accordance with Paragraphs 8, 9 and 10 of Framework Schedule 3.

REIMBURSABLE EXPENSES
None

DISBURSEMENTS
Any disbursements must be agreed in advance by the Buyers Contract Manager.

For the avoidance of doubt, if the Buyers Contract Manager agrees that the Suppliers shall instruct Counsel, the Supplier shall instruct Panel Counsel at Panel Counsel rates.

ADDITIONAL TRAINING CHARGE
None

SECONDMENT CHARGE
This will be agreed in the event that a secondment is requested (see Specification).

PAYMENT METHOD
Draft invoices with full narrative to include work to that point should be sent to Amir Mughal by 5 working days before the end of the month for approval. Once the draft invoice is approved, the invoice should be sent to the Buyer's Invoicing Address quoting the correct Purchase Order Number.

Payment will be made by Bank Transfer.

BUYER'S INVOICING ADDRESS:
[redacted]
[redacted]- COVID-19 Inquiry Response Unit
[redacted]
1 Victoria Street, London, SW1H 0ET

BUYER'S AUTHORISED REPRESENTATIVE(S)
[redacted]
[redacted] Director
[redacted]
1 Victoria Street, London, SW1H 0ET

[redacted]
Senior Lawyer
[redacted]
Covid Public Inquiry Team,
Government Legal Department,
102 Petty France
Westminster

London
SW1H 9GL

BUYER'S ENVIRONMENTAL POLICY
Available on request

BUYER'S SECURITY POLICY
Available on request

BUYER'S ICT POLICY
Available on request

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]
[redacted], Head of Public Inquiries and Public Law Team
[redacted]
20 Gresham Street, London, EC2V 7JE

SUPPLIER'S CONTRACT MANAGER
[redacted]
[redacted], Head of Public Inquiries and Public Law Team
[redacted]
20 Gresham Street, London, EC2V 7JE

PROGRESS REPORT
See Call-Off Schedule 20

PROGRESS REPORT FREQUENCY
As requested by the Buyers Authorised Representative, but no less frequent than monthly.

PROGRESS MEETINGS AND PROGRESS MEETING FREQUENCY
As requested by the Buyers Authorised Representative, but no less frequent than monthly.

KEY STAFF

[redacted]
[redacted], Head of Public Inquiries and Public Law Team
[redacted]
20 Gresham Street, London, EC2V 7JE

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
Not applicable

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	[redacted]	Role:	[redacted]
Date:	20 July 2022	Date:	21/07/22

Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance and forward plan	As requested	As requested	As requested
Call-Off Contract Charges and budget management	As requested	As requested	As requested
Key Subcontractors	As requested	As requested	As requested
Technical	As requested	As requested	As requested
Performance management	As requested	As requested	As requested

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	N/A	**TLT's Fee Rates** TLT's Legal Services Panel framework rates were negotiated by TLT on entry to the CCS' Legal Services Panel. Where applicable, TLT may also have negotiated alternative fee arrangements and discounted rates with clients. If these rates were disclosed, and became known to competitors and/or the wider legal market, it would inhibit TLT's ability to engage with future bid and tender processes, as it would give our competitors a competitive advantage. It would therefore be likely to prejudice the ability of TLT to participate competitively in the market. *This item should be read to include any information extracted from the TLT framework fee rate card and/or included in any email correspondence and/or other documents that reference the rates of TLT's lawyers.*	Indefinite

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with

UK GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the

requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

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

1.1 The contact details of the Relevant Authority's Data Protection Officer are: [redacted]

[redacted]plier's Data Protection Officer are: [redacted];

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of, for example, the Supplier:* ● *Providing legal and strategic advice and support on specific issues and providing general legal and administrative support;* ● *Advising and supporting in the disclosure and review of documentary evidence;* ● *Advising and supporting in the preparation of evidential material and/or otherwise assisting in the provision of such material to the Inquiry in accordance with any request or requirement by the Inquiry;* ● *Advising and supporting in the representation of the Relevant Authority, via counsel, at Inquiry hearings;* ● *Advising and supporting in preparation for the publication of the Inquiry's reports and Rule 13 warning letters;*
Duration of the Processing	31 March 2025 OR on completion of the Deliverables

Nature and purposes of the Processing	*Provision of legal services which may involve the processing of personal data. The data may be provided by the Relevant Authority, or related third parties, be stored on the Supplier's storage systems, used for the purposes of the provision of legal services to the Relevant Authority and deleted in accordance with the Supplier's data retention policy or by the instruction of the Relevant Authority in accordance with the statutory, and related common law, obligations of the Relevant Authority.*
Type of Personal Data	*Names, addresses, dates of birth, telephone numbers, pay, images, email addresses, professional information, racial or ethnic origins, political opinions, religious or philosophical beliefs, Trade Union membership, health, sex life or sexual orientation, children's data, criminal data.*
Categories of Data Subject	*Staff (including volunteers, agents, and temporary workers and former employees) customers/ clients, suppliers, patients, members of the public and other third parties,*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*The data may be deleted in accordance with the Supplier's data retention policy and/or by the instruction of the Relevant Authority in accordance with the statutory, and related common law, obligations of the Relevant Authority.*

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Relevant Authority:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every 6 months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. **Audit**

4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's

data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by

the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of

compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

1 Background

1.1. On 12 May 2021 the Prime Minister announced a statutory public inquiry into the State's actions during the COVID 19 pandemic. The Inquiry is due to begin in spring 2022.

1.2. The draft Terms of Reference for the Inquiry were published on 10 March 2022. The Inquiry will examine issues of exceptional public interest, weight and complexity and will inevitably involve significant press interest. The draft Terms of Reference are very broad in scope, covering: preparedness; the public health response; the response in the health and care sector; and the economic response.

1.3. The Prime Minister has acknowledged the large amount of resources that will be involved in the months of preparation for the Inquiry and the potentially large amount of time which will be spent by people testifying in public.

1.4. As such, each Government Department is likely to be expected to contribute to the Inquiry, and a number of these have been working with GLD to prepare for the work required. GLD anticipates that it will need external law firms to provide additional resource and expertise to support the departments, and this Call Off Contract has been established between the Buyer and the Supplier to provide this support.

2. **Purpose of the Call Off Contract**The Supplier shall provide legal support to the Buyer in addition to that provided by GLD, in its response Covid inquiry.

2.2. We envisage GLD, the Supplier and every firm appointed to support other government Departments collaboratively working together, in order to provide a seamless and cost effective service for clients. The scale of the Inquiry is likely to require a flexible and innovative approach, including the potential for firms working together in partnership where appropriate.

3. The general approach

3.1. GLD will provide the recognised legal representative (RLR) to the Inquiry as required under the Inquiries Act 2005 for each department.

3.2. The GLD RLR will be the point of contact for the Buyer and the Supplier.

3.3. The GLD RLR will procure any necessary e-disclosure system for the Buyer, and the Supplier will use this, where required, in provision of the Services and Deliverables.

3.4. The GLD RLR, as well as drawing on wider GLD support, will be able to instruct the Supplier to undertake specific tasks in support of their role as RLR in consultation with the Buyer. For example:

3.4.1. Providing legal and strategic advice and support on specific issues and providing general legal and administrative support;

3.4.2. Advising and supporting in the disclosure and review of documentary evidence;

3.4.3. Advising and supporting in the preparation of evidential material and/or otherwise assisting in the provision of such material to the Inquiry in accordance with any request or requirement by the Inquiry;

3.4.4. Advising and supporting in the representation of the department, via counsel, at Inquiry hearings;

3.4.5. Advising and supporting in preparation for the publication of the Inquiry's reports and Rule 13 warning letters;

3.5. The GLD RLR will be responsible for the relationship with the Supplier, including but not limited to, checking the quality of work and the accuracy and reasonableness of invoices.

3.6. The GLD RLR will instruct any counsel required to represent the Buyer. Where the Supplier wishes to instruct additional counsel to assist with a task, for example disclosure, this instruction will be subject to the GLD RLR's prior approval and managed through them.

3.7. The GLD RLR will sign off, once the Buyer is content, all external communications with or related to the Inquiry.

3.8. The GLD RLR will advise the Buyer on the strategic approach, and will attend where necessary internal cross–government meetings, to ensure consistency of HMG approach.

4. Instructions

4.1. Where the Buyers Authorised Representative has a request for a "work package" of Services under this Call Off, they will send an email to the Supplier with the request. The Supplier and the Buyer will then agree the scope and detail of the Services, Deliverables and the timescales and fee estimate for the work. This agreement will be confirmed in writing between the Parties.

4.2. Where the Buyer requires

4.2.1. Call Off Special Term 1 (Conflicts Waiver); and/or

4.2.2. Call Off Schedule 9 (Security) Part A or B; and/or

4.2.3. Call Off Schedule 26 (Non Disclosure Agreement)

to apply, this shall be set out in the agreement for those Services

4.3. In the event that the Buyer requires Services under Scottish Law, Call Off Schedule 19 (Scottish Law) will apply to that request under this Call Off Contract.

4.4. In the event that the Buyer requires Services under Northern Irish Law, Call Off Schedule 21 (Northern Irish Law) will apply to that request under this Call Off Contract.

5. Progress Reports and Progress Meetings

5.1. The content and format of any progress reports will be agreed by the parties, but are likely to include work completed but not yet invoiced, progress on current work packages, forecast spend against budget, forward look of activity, risks and issues arising.

5.2. In addition to meetings to discuss the provision of the Services, progress meetings may include meetings with other government Departments and their legal advisors in relation to the provision of advice to government for the Inquiry.