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

Order Form

CALL-OFF REFERENCE:	con_3321
THE BUYER:	**Department for Business, Energy and Industrial Strategy (on behalf of The Post Office Horizon IT Inquiry)**
BUYER ADDRESS	1 Victoria Street, London, SW1H 0ET
THE SUPPLIER:	TLT LLP
SUPPLIER ADDRESS:	One Redcliff, Street Redcliff, Bristol, BS1 6TP
REGISTRATION NUMBER:	OC308658
DUNS NUMBER:	**72-928-1603**
SID4GOV ID:	**Not Applicable**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 9th December 2022.
It is issued under the Framework Contract with the reference number Legal Services Panel RM6179 for the provision of legal advice and services.

CALL-OFF LOT(S):
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. 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 con_3321
     - Call-Off Schedule 1 (Transparency Reports)
     - Call-Off Schedule 2 (Staff Transfer)
     - Call-Off Schedule 3 (Continuous Improvement)
     - Call-Off Schedule 5 (Pricing Details)
     - Call-Off Schedule 7 (Key Supplier Staff)
     - Call-Off Schedule 20 (Call-Off Specification)
     - Call-Off Schedule 24 (Special Schedule)
4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6179
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.

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:

None

CALL-OFF START DATE: **09 December 2022**

CALL-OFF EXPIRY DATE: **28 Feb 2023**

CALL-OFF INITIAL PERIOD: **28 working days**

CALL-OFF MAXIMUM CONTRACT VALUE: **£630,140 (excluding VAT)**

CALL-OFF OPTIONAL EXTENSION PERIOD: Not Applicable

WORKING DAY
Standard business working days

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
When submitting a bid, a conflict of interest statement is needed from all suppliers, this includes steps they are taking or will take to manage potential or perceived conflicts of interest. The quality of these mitigating steps or how the conflict of interest will be managed will be a discussion with the successful supplier depending on the conflict on interest (if there is any) and mitigating actions.
Staff working on the contract will also need to complete conflict of interest declarations.
The successful supplier is also bound by the clause 32 and its sub clauses in the core terms.

CONFIDENTIALITY
All parties working on this contract will be required to sign confidentiality undertakings. These will ensure that any material seen by the supplier can be used only for the purposes of this contract. For the successful supplier all information seen, provided, accessed, assumed, deduced or generated under the work should be assumed confidential, and covered by the personal confidentiality undertaking. Information obtained in confidence during the contract must not be disclosed to a third party without prior consent of the buyer. Such information is also bound by clause 15 (and its sub clauses) in the core terms.

IPR
In alignment with clause 9 of the Core Terms

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.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£630,140.00**

CALL-OFF CHARGES
See details in Call-Off Schedule 5 (Pricing Details)

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
Not payable

ADDITIONAL TRAINING CHARGE
None

SECONDMENT CHARGE
Not applicable

PAYMENT METHOD
Payments will be linked to delivery of key milestones. BEIS aims to pay all correctly submitted invoices as soon as possible with a target of 10 days from the date of receipt, via BACS and within 30 days at the latest in line with standard terms and conditions of contract.

BUYER'S INVOICING ADDRESS:
The Department for Business, Energy and Industrial Strategy (on behalf of the Post Office Horizon Inquiry Secretary)
[redacted]
c/o
1 Victoria Street, Westminster, London, SW1H 0ET

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]

BUYER'S CONTRACT MANAGER
[redacted]

BUYER'S ENVIRONMENTAL POLICY
Available upon request

BUYER’S SECURITY POLICY

Available upon request

BUYER'S ICT POLICY
Available upon request

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

SUPPLIER'S CONTRACT MANAGER
[redacted]

PROGRESS REPORT
Reporting is as set out in the specification

PROGRESS REPORT FREQUENCY
Reporting is as set out in the specification

PROGRESS MEETINGS AND PROGRESS MEETING FREQUENCY
Meetings and frequency are as set out in the specification

KEY STAFF
[redacted]

[redacted]

KEY SUBCONTRACTOR(S)
Not Applicable

COMMERCIALLY SENSITIVE INFORMATION
Supplier's Commercially Sensitive Information

SERVICE CREDITS
Not applicable
A Critical Service Level Failure is:
The supplier fails to respond to feedback on quality (including accuracy and speed of delivery) of throughput and continues producing work below standard.
The supplier fails to respond to meet agreed throughput targets (as outlined in specification or agreed separately) and produces insufficient work.
The supplier misses an agreed deadline as outlined in the specification.
A risk log produced on the outset and set up of the project. Risks not being managed effectively to mitigate issues by the supplier.

Risks are those that could cause (1) commercial impact, (2) reputational impact (3) legal impact and (4) delivery impact or (5) any other significant impact not covered in (1)-(4).

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)

Signature Area

(dd.mm.yyyy | hh:mm:ss)

Organisation Name:
Department for Business, Energy & Industrial Strategy

Role/Title:
[redacted]

Name:
[redacted]

Signature: [redacted]

15 January 2023 | 21:53:30 GMT

Organisation Name:
TLT LLP

Role/Title:
[redacted]

Name:
[redacted]

Signature: [redacted]

15 January 2023 | 19:19:29 GMT

(dd.mm.yyyy | hh:mm:ss)

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
	N/A		

1			[redacted] [redacted] [redacted] [redacted]	Indefinite

Signature Area

(dd.mm.yyyy | hh:mm:ss)

Organisation Name:
Department for Business, Energy & Industrial Strategy

[redacted]

Name:
[redacted]

Signature [redacted]

15 January 2023 | 21:53:30 GMT

Organisation Name:
TLT LLP

Role/Title:
[redacted]

[redacted]

Signature: [redacted]

15 January 2023 | 19:19:29 GMT

(dd.mm.yyyy | hh:mm:ss)

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: BEIS Data Protection Officer, Department for Business, Energy & Industrial Strategy (BEIS), 1 Victoria Street, London SW1H OET. Email [redacted]

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted] - 20 Gresham Street, London EC2V 7JE. Email: [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 Of Authorised Processing	**Details**
Identity of the Controller and Processor	Each Party is an independent controller of the following Personal Data which it receives: • Stakeholder names, business telephone numbers and email addresses, office location and organisational roles of either party and other external parties (such as other advisers)
Use of Personal Data	Management of this Legal Services Contract and any case of claim supported under it.
Subject matter of the processing	Processing is required to ensure that the supplier can effectively deliver the contract and provide a service to the buyer. Processing is also required by the supplier to enable the buyer to fulfil its statutory obligations and functions under the Inquiries Act 2005.
Duration of the processing and retention.	From the outset of the Legal Services Contract date, and up to 7 years after it expires.

Nature and purposes of the processing	Provision of legal services under this Legal Services Contract. The buyer is (i) a Statutory Inquiry under the Inquiries Act 2005 exercising functions in the public interest, and (ii) a data controller, and has decided the means and purposes of why personal data is needed. The supplier shall process data as required and instructed by the buyer, to undertake its duties and fulfil its obligations under this Framework Agreement. The nature and purposes for which the Inquiry processes personal data is to enable the Inquiry to: i. discharge its obligations in its published Terms of Reference ii. exercise its statutory functions as conferred upon it by an enactment/rule of law (The Inquiries Act 2005, The Inquiry Rules 2006) iii. comply with its legal obligations in the exercise of the Inquiry’s official authority (e.g., Public Records Act 1958, The Data Protection Act 2018, The Freedom of Information Act 2000, The Inquiries Act 2005, The Inquiry Rules 2006 and the General Data Protection Regulations) iv. satisfy the substantial public interest in the Inquiry v. to assist with recruitment of new Review Team members if and when required The nature of the processing includes but is not limited to any operation such as receipt, collection, recording, organisation, copying, structuring or restructuring, storage, adaptation or alteration, retrieval, consultation and analysis, disclosure, transmission, dissemination, or otherwise making accessible or available, alignment or combination, configuring, reconfiguring, or combining, restricting, erasure or destruction of data (whether or not by automated means).

Type of Personal Data	**Staff of either Party:** Full name Workplace address Workplace Phone Number Workplace email address Date of Birth Photocopy of ID documents **Personal data which is the subject of the transaction:** • Personal data – typically biographical data such as name, date of birth, personal description, contact details, images (photographs) and voice recordings (including camera recordings) but may also include other identifiers, marital status and dependents (including children and vulnerable adults), nationality, and gender. • It may also include the employment records of any of the persons listed under “Categories of Data Subject” below. • It may also include consultation and survey responses, information relating to compensation, mediation and grievance, and Non-Disclosure Agreements • Special category data – Processing by the Inquiry potentially extends to all types of special category personal data, but most typically will involve information relating to health, race/ethnicity, religious beliefs and trade union membership. • Personal data relating to criminal convictions and offences – typically this may include detail of the offence, sentencing remarks, the period of sentence and/or any other sanction imposed by the criminal courts, such as a fine or community service.
Categories of Data Subject	Staff of either Party Personal data processed by the supplier can comprise the personal data of: • Members of the public who contact the Inquiry

	• Core Participants in the Inquiry • Other witnesses providing evidence to the Inquiry • Contracted parties to the Inquiry • Persons referred to in information received by the Inquiry from any of the above. • Dependents of any of the above (including children and vulnerable adults).
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	Personal data will be held by the Inquiry until the conclusion of the Inquiry. At the end of the Inquiry, some of the personal data held by the Inquiry will – where it is considered to form part of the historic record – be transferred for the purposes of indefinite retention of Inquiry records by the National Archives in accordance with the Public Records Act 1958. Any personal data included will continue to be protected. Personal data that is not required for archiving purposes will be destroyed.
Controls in place to prevent further use of the data	The Inquiry has appropriate technical and organisational measures in place with its data processors, which means they cannot do anything with a data subjects' personal information unless the Inquiry, as Data Controller, has instructed them to do so (see below). The data processor will not share personal information with any organisation apart from the Inquiry, or as directed by the Inquiry, and will hold the data securely and retain it only for the period the Inquiry requires. Typically, personal data is held in digital format in IT systems which meet government security standards. The details of the security arrangements are not set out here to avoid compromising the effectiveness of those arrangements, but measures outlined are mentioned below. Technical measures include but are not limited to; encryption and password protection which determine, control and authenticate access to IT systems, networks, hardware and software, firewalls, up to date operating systems and security patches, back-up and recovery in the event of system failure, disaster, data corruption or data breach, and quarantining Inquiry files from wider shared systems.

Organisational measures include but are not limited to: assessing risk and maintaining a risk register, mandatory staff training on GDPR and Data Breaches, the appointment of a Data Protection Officer to support the Inquiry’s compliance with relevant data protection obligations and to proactively manage any risks, and policies and procedures for records and information management such as; a Privacy Notice, Protocol on the Disclosure of Documents, Protocol on Redaction, Anonymity and Restriction Orders, and Appropriate Policy (sensitive & criminal data handling).

As personal data is stored on the Inquiry’s IT infrastructure, and shared with its data processors, that data may be transferred and stored securely outside the European Union. Where that is the case, all appropriate technical and legal safeguards will be put in place to ensure data subjects are afforded with same level of protection.

Personal data will be held by the Inquiry until its conclusion. At which point data considered to form part of the historic record will be transferred to the National Archives for indefinite retention in accordance with the Public Records Act 1958. Any personal data included will continue to be protected. Personal data that is not required for archiving purposes will be securely destroyed

Signature Area

(dd.mm.yyyy | hh:mm:ss)

Organisation Name:

Department for Business, Energy & Industrial Strategy

Role/Title:

[redacted]

Name:

[redacted]

Signature: [redacted]

15 January 2023 | 21:53:30 GMT

Organisation Name:
TLT LLP

Role/Title:
[redacted]

Name:
[redacted]

Signature [redacted]

15 January 2023 | 19:19:29 GMT

(dd.mm.yyyy | hh:mm:ss)