RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	TROP0089
THE BUYER:	Department for Transport (DfT)
BUYER ADDRESS	33 Horseferry Road, Westminster, London SW1P 4DR
THE SUPPLIER:	KPMG LLP
SUPPLIER ADDRESS:	15 Canada Square, London, E14 5GL
REGISTRATION NUMBER:	OC301540
DUNS NUMBER:	423916167
SID4GOV ID:	N/A

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated: 6 August 2024

It's issued under the Framework Contract with the reference number RM6187 for the provision of Financial Advisors to support Rail Contracts & Projects

CALL-OFF LOT(S): LOT 4

Call-off incorporated terms

The following documents are incorporated into this Call-Off Contract.

Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187
3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility)
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**.**

Supplier terms are not 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:

[redacted]

Call-off start date: 12 August 2024

Call-off expiry date: 11August 2027

Call-off initial period: 3 years

Call-off Optional Extension Period: Initial period for 3 years with an option to extend for 1 year at the Authority's sole discretion. End date of extension period: 11 August 2028

Call-off deliverables:

As per Attachment 3 – Statement of Requirements

Security

Short form security requirements apply

DfT takes data security extremely seriously and applies agreed government security procedures to all Contracts involving the handling of data and 'Official Sensitive' and 'Commercial Sensitive' information.

DfT requires that the Advisor treats confidentially all information provided and procured under this contract and that this obligation survives the duration of this contract. DfT requires that the Advisor produces and maintains robust processes, systems and controls to ensure information provided and produced under this contract is not shared with third parties or utilised by the Advisor to the benefit of third parties or to the detriment to DfT.

The Advisor is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of the Rail Transformation Programme, including, as necessary, limits on access to IT systems and password protections. There will be serious consequences should any information make its way to the public domain.

With regard to Intellectual Property Rights (IPR), DfT will have ownership of any outputs that are produced under this contract. Any outputs produced under this contract may be publicly available and may be used by DfT at its own discretion. It is expected that all deliverables will be provided to DfT via an agreed method of transfer in order for DfT to use these in future and/or for exit purposes.

Advisors are to note that all staff they supply or intend to supply who have regular access to or will be based at the Authorities premises have complied with the Authorities baseline personnel Security Standard (BPSS) (https:/www.gov.uk/government/publications/security-policy-framework).

Maximum liability

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

As there is no overall contract value assigned for this call-off contract, the maximum liability for the whole duration of the call-off contract will be £4m.

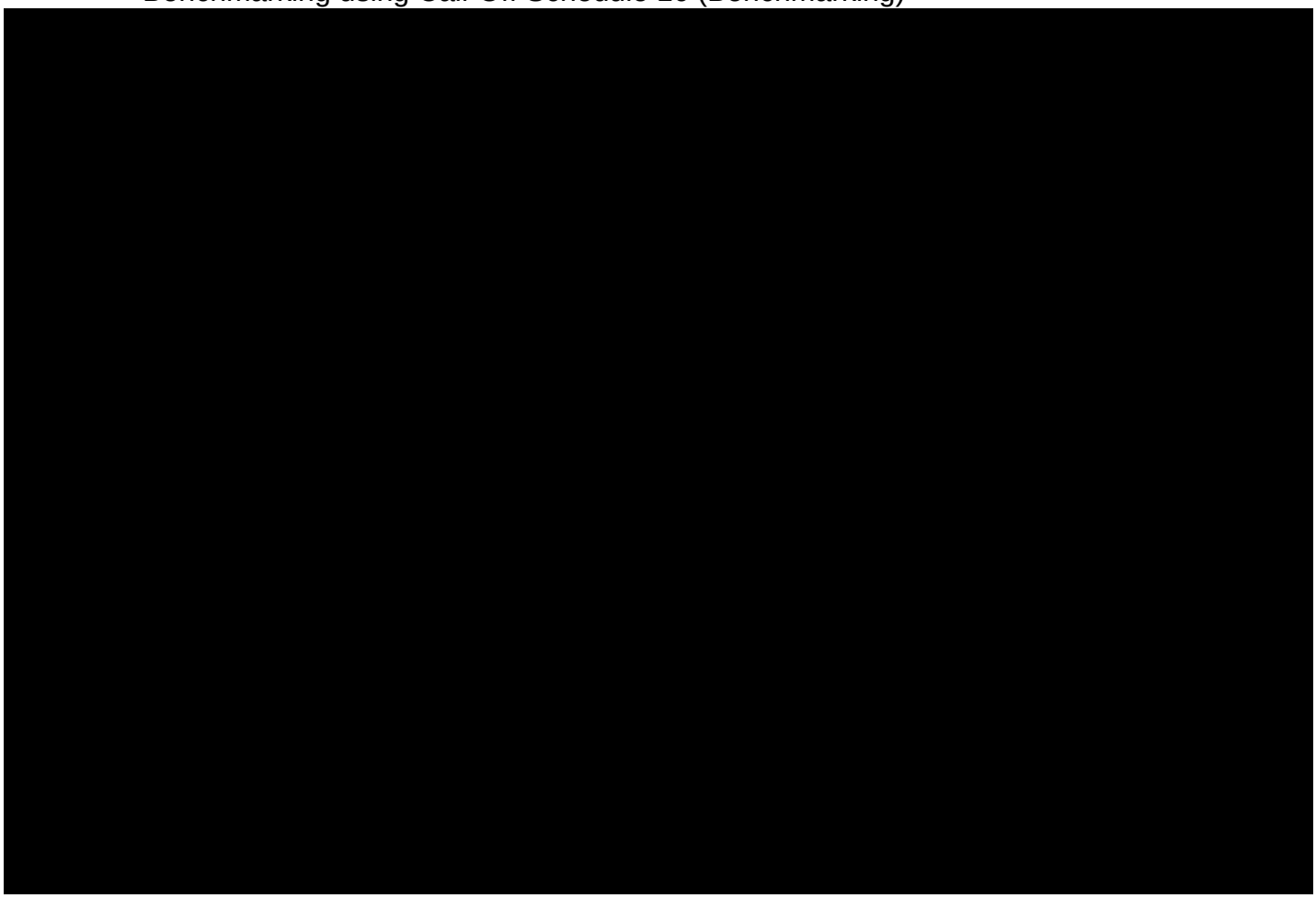
Call-off charges

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

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law
- Benchmarking using Call-Off Schedule 16 (Benchmarking)



Reimbursable expenses

Attendance at Contract Review meetings shall be at the Advisor's own expense. DfT will not pay for meeting rooms and other associated expenses.

Payment method

BACS

Buyer's invoice address

[redacted]

FINANCIAL TRANSPARENCY OBJECTIVES
The Financial Transparency Objectives do not apply to this Call-Off Contract.

Buyer's authorised representative

[redacted]

Buyer's security policy

Please see Annex 2

Supplier's authorised representative

[redacted]

Supplier's contract manager

[redacted]

Progress report frequency

The Advisor is expected to deliver progress reports monthly and as may be reasonably required by DfT from time to time (subject to any alternative arrangements being reached) for any Statement of Works (SoW) they have. Such reports would be expected to cover the following areas:

- Progress on SoWs
- Forward plan on activities per SoW
- Forecast completion dates for SoW activities
- Key risks and emerging issues impacting progress with planned or existing mitigations where relevant
- Progress with regards to milestones and deliverables made in the previous month
- Financial progress, including costs incurred to date and forecast costs to the end of any particular activity (SoW). This should include a detailed breakdown on activity

completed by grade, name of the person who has carried out the work, their daily rate and the total number of days charged for each respective SoW.

- Quarterly reports on knowledge transfer/lessons learned (this can include case studies etc.)
- Exit plan to be produced at the start of the contract and updated annually with the final version in place 1 year before end of the contract. This is to be shared with Group Commercial and the Contract Management Team (CMT) which sits within PTLG and RISDG. Draft exit plan to be sent to DfT within one month of contract start date.

Progress meeting frequency

The Contract Management Team (CMT) is the overall Contract Manager responsible for overseeing the day-to-day administration of this contract.

Contract management reviews will be held regularly if any call-offs have been commissioned at pre-agreed dates and locations/Teams meeting and will include discussions on progress of SoWs. These reviews will be conducted by individual project teams and the CMT to ensure oversight and understanding of the work being delivered.

Advisors will be expected to attend individual project introduction meetings, to discuss future relationships and expectations.

Advisors will be expected to participate in Contract Management Meetings for each SoW that has been allocated to them.

All SoWs will be published to the relevant Advisor via the e-sourcing portal, Jaggaer, and successful Advisors are expected to review and provide a price proposal using this portal. KPIs will also be reviewed and monitored through the e-sourcing portal and successful advisors will be required to update their scorecards each month for any live call-offs. These will be discussed at contract management meetings.

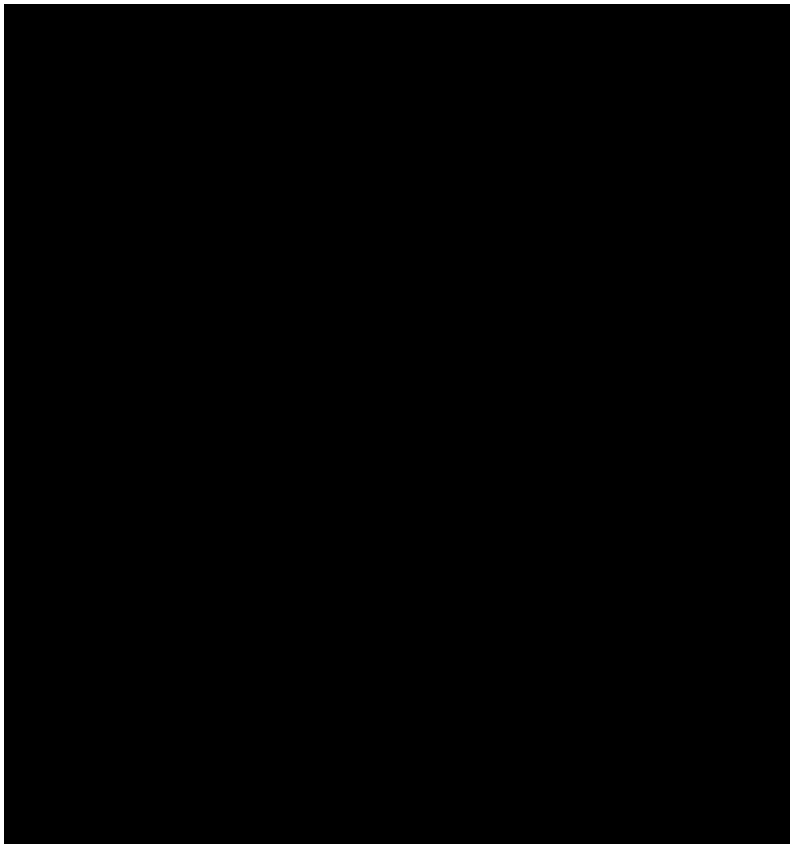
Attendance at Contract Review meetings shall be at the Advisor's own expense.

DfT will appoint Contract Managers to manage the individual SoWs. These will be from the individual project teams.

Key staff

[redacted]

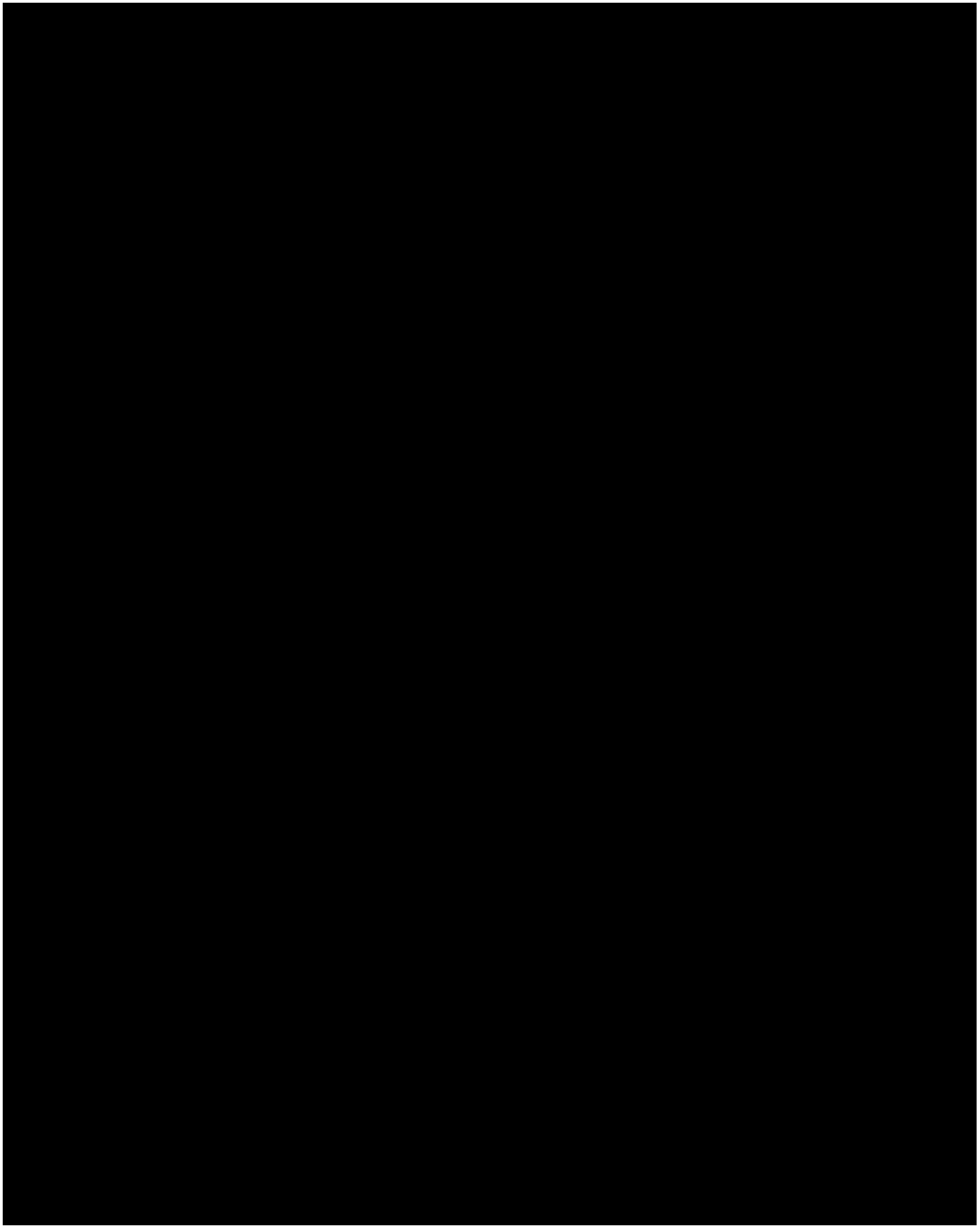
Key subcontractor

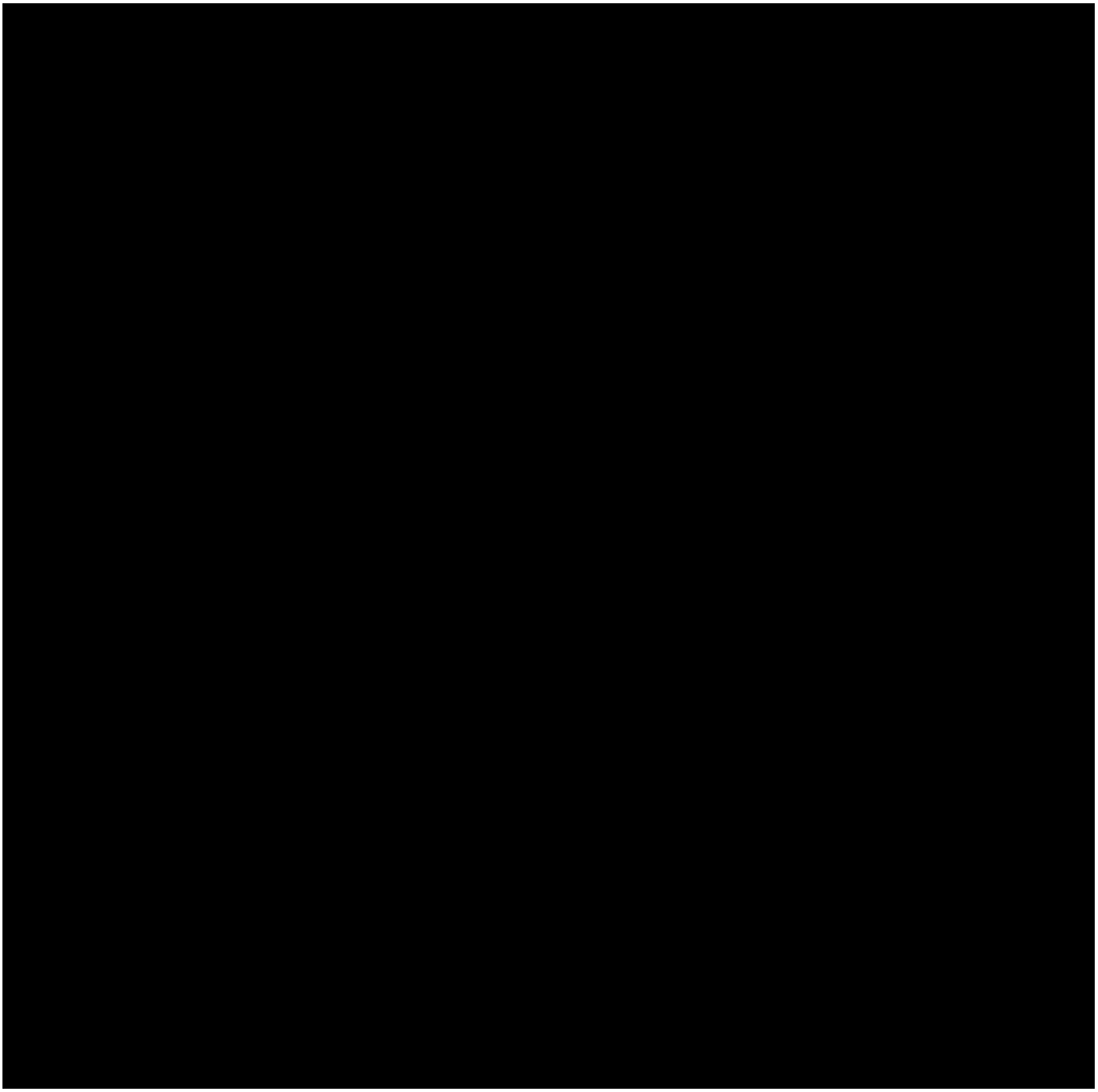


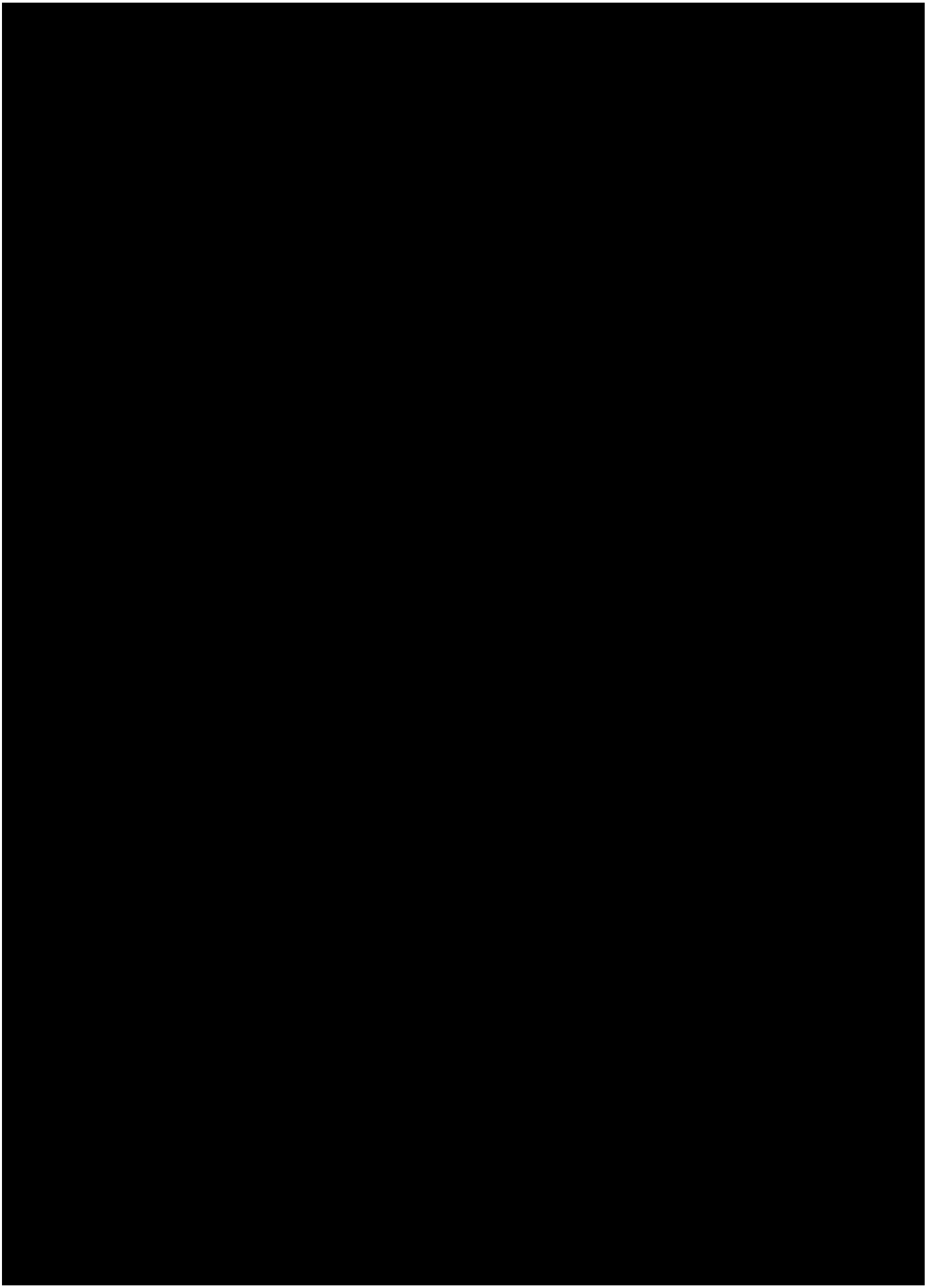
Commercially sensitive information
Please see Security section

Key Performance Indicators

Please see below







Additional insurances
Not applicable

Guarantee
Not applicable

Buyer's environmental and social value policy

Please see Annex 3

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)]

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Supplier:

For and on behalf of the Buyer:

Joint Schedule 11 (Processing Data)

Definitions

o 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

o 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:

- "Controller" in respect of the other Party who is "Processor";
- "Processor" in respect of the other Party who is "Controller";
- "Joint Controller" with the other Party;
- "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

o 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.

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

o 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 systematic description of the envisaged Processing and the purpose of the Processing;
- an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
- an assessment of the risks to the rights and freedoms of Data Subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

- The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
  - 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;
  - 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:
    - nature of the data to be protected;
    - harm that might result from a Personal Data Breach;
    - state of technological development; and
    - cost of implementing any measures;
  - ensure that :
    - the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
    - 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:
      - 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;
      - are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
      - 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
      - have undergone adequate training in the use, care, protection and handling of Personal Data;
  - not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
    - 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;
    - the Data Subject has enforceable rights and effective legal remedies;
    - 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

- 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

- 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.

- 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:

- receives a Data Subject Access Request (or purported Data Subject Access Request);
- receives a request to rectify, block or erase any Personal Data;
- receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
- 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
- becomes aware of a Personal Data Breach.

- 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.

- 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:

- the Controller with full details and copies of the complaint, communication or request;
- 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;
- the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- assistance as requested by the Controller following any Personal Data Breach; and/or
- 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.

- 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:

- the Controller determines that the Processing is not occasional;

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

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

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

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

- notify the Controller in writing of the intended Subprocessor and Processing;
- obtain the written consent of the Controller;
- 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
- provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

o 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).

o 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

o 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

o 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.

o 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.

- 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.

- 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.

- The Parties shall only provide Personal Data to each other:

  - to the extent necessary to perform their respective obligations under the Contract;

  - 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

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

- 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.

- 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.

- 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")**:

  - 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

  - 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:

    - 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

    - 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.

- 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:

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

  - implement any measures necessary to restore the security of any compromised Personal Data;

  - 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

  - 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.

- 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).*

- 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)*.

- 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.

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

The contact details of the Supplier's Data Protection Officer are: [redacted]

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller
Duration of the Processing	For the duration of the Framework Contract plus 7 years
Nature and purposes of the Processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data	• Full name • Workplace address • Workplace Phone Number • Names • Job Title • Compensation • Tenure Information Qualifications or Certificate • Nationality

	• Education and Training History • Personal Interests • References and referee details • National Insurance Number • Bank statement • Utility bills • Job title or role • Job application details • Start date • End date and reason for termination • Contract type • Compensation data • Photographic Facial Image • Biometric data • Birth certificates • IP address • Details of physical and Psychological health or medical condition • Next of kin & emergency contact details • Record of absence, time tracking & annual leave
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public
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	For the duration of the Framework Contract plus 7 years