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

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Deliverables and dated 01 December 2025. It is issued under the Framework Contract with the reference number RM6309.

SECTION 1: CONTRACTING PARTIES

CALL-OFF REFERENCE:	P11889
THE BUYER:	Cabinet Office
BUYER ADDRESS	70 Whitehall, London, SW1A 2AS
THE SUPPLIER:	Soteria International Ltd t/a Soteria Consulting Ltd
SUPPLIER ADDRESS:	**37 St John Road, Sidcup, Kent. DA14 4HD**
REGISTRATION NUMBER:	**06647104**

SECTION 2: CALL-OFF CONTRACT TERM

CALL-OFF START DATE:	29 December 2025
CALL-OFF EXPIRY DATE:	29 March 2026
CALL-OFF INITIAL PERIOD:	3 months
CALL-OFF OPTIONAL EXTENSION PERIOD	1 month

SECTION 3: CALL-OFF DELIVERABLES

Deliverables include:

1. Research report comparing the GCO reward framework with that in place in the private sector
2. Costed options for reform to the current reward framework
3. Proposed governance and accountability framework
4. Communications and change guidance
5. Proposed implementation plan.

See Annex 1 for the full Statement of Requirement.

SECTION 4: CALL-OFF CHARGES

The call off charges are a fixed price of £74,000 (excl VAT) to deliver the Deliverables.

SECTION 5: PAYMENT METHOD

The payment method is via Bacs on receipt of valid invoice.

SECTION 6: BUYER AND SUPPLIER DETAILS

BUYER'S INVOICE ADDRESS:

Invoices should be submitted to: REDACTED TEXT under FOIA Section 40, Personal Information

A copy of the invoice should also be sent to REDACTED TEXT under FOIA Section 40, Personal Information

BUYER'S AUTHORISED REPRESENTATIVE
REDACTED TEXT under FOIA Section 40, Personal Information

SUPPLIER'S AUTHORISED REPRESENTATIVE
REDACTED TEXT under FOIA Section 40, Personal Information

SUPPLIER'S CONTRACT MANAGER
REDACTED TEXT under FOIA Section 40, Personal Information

SECTION 9: COMMERCIALLY SENSITIVE INFORMATION

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

SECTION 10: BUSINESS CONTINUITY DISASTER RECOVERY PLAN

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

SECTION 11: 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

2. Joint Schedule 1 (Definitions)
3. Framework Special Terms
4. The following Schedules will be included in equal order of precedence:
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 6 (Key Subcontractors)
    - Joint Schedule 7 (Financial Difficulties)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)
    - Call-Off Schedule 7 (Key Supplier Staff), if required section 6 of the short Order Form should be populated
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 14 (Service Levels)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility)
7. 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.

SECTION 12: CALL-OFF SPECIAL TERMS

LIMITATION OF LIABILITY

12.1 Notwithstanding Clauses 11.2 and 11.6 of the Core Terms, the total aggregate liability of the Supplier arising under or in connection with this Call-Off Contract (whether in tort, contract, or otherwise) shall not exceed an amount equal to 100% of the total Charges paid or payable under this Contract (being £74,000 excluding VAT).

12.2 For the avoidance of doubt, the Data Protection Liability Cap referred to in Clause 11.6 of the Core Terms shall be £74,000.

12.3 The liability cap in Clause 1.1 above shall apply to all claims arising under this Contract, including (but not limited to) claims under the indemnities at Clauses 9.5 and 14.8(e) of the Core Terms, save only for liability arising from the Supplier's fraud or wilful misconduct.

12.4 The supplier’s liability under the indemnities at Clause 7.5, 31.3, and Call-Off Schedule 2 (if applicable) of the Core Terms shall

be subject to the overall liability cap set out in Clause 1.1 above, save only for liability arising from the Supplier's fraud or wilful misconduct.

INTELLECTUAL PROPERTY

12.5 The Supplier may reference the work conducted under this Contract (in anonymised form) in case studies, proposals, and marketing materials, subject to the Buyer's prior written consent (such consent not to be unreasonably withheld or delayed.

SECTION 13: MAXIMUM LIABILITY

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£74,000.**

SECTION 14: REIMBURSABLE EXPENSES

None

SECTION 15: SERVICE CREDITS

None

SECTION 16: PROCESSING DATA

The Buyer must confirm the following statements:

That the Buyer has reviewed Joint Schedule 11 (Process Data) Yes
That Annex A has been completed by the Controller where applicable Yes ● The roles for the processing of data under this Call-Off Contract will be:

Buyer:- Controller

Supplier: Processor

SECTION 17: SECURITY

Part A: Short Form Security Requirements from Call Off Schedule 9 (Security) is applicable to this short Order Form.

Signed - via Docusign
Supplier Soteria International Group Ltd ta Soteria Consulting <Supplier Sign Here>
REDACTED TEXT under FOIA Section 40, Personal Information 12/22/2025
Buyer Cabinet Office <Commercial Sign Here>
REDACTED TEXT under FOIA Section 40, Personal Information 12/22/2025

Annex 1: The Statement of Requirement

1. PURPOSE

1.1 The purpose of this procurement is to appoint a supplier to deliver a review of the Government Commercial Organisation (GCO) reward framework. The supplier will provide an evidence-based analytical report, including case studies, of how GCO's reward framework compares to the external market. The report will include proposals to reform the framework, ensuring it's competitive, fair, transparent, and aligned with government objectives.

1.2 By Framework we mean both the structures in place, the policies and the governance.

2. BACKGROUND TO THE BUYER

2.1 The Government Commercial Organisation (GCO) was established in 2016–17 as the single employer for senior commercial professionals across government. Its objectives are to attract, develop and retain world-class talent, and to ensure the commercial function delivers best value for the taxpayer. Employees transitioned to GCO from departmental roles from April 2017, operating under bespoke GCO terms (higher salary, Performance-related Pay (PRP), reduced pension/leave) or Civil Service Equivalent terms.

3. BACKGROUND TO REQUIREMENT /OVERVIEW OF REQUIREMENT

3.1 GCO's reward framework has remained static since inception and is considered misaligned with external markets and internal expectations. It is therefore believed to be impacting recruitment and retention, where we expect there to be future risks arising in digital, including AI, nuclear and future-focused roles.

3.2 Employee expectations around salary, PRP and overall total reward have also become misaligned with original policy intent.

3.3 A review of GCO's reward arrangements is required to benchmark GCO's policies, approaches and pay data against comparators to generate reform options.

4. DEFINITIONS

	Expression or Acronym Definition
PRP	Performance-Related Pay, Element of variable pay, paid annual linked to performance
Annual short-term incentive scheme Pay Comprises	salary and allowances

5. SCOPE OF REQUIREMENT

5.1 In Scope:

- Review of GCO reward framework, the structures and how they operate including:
- All GCO commercial and procurement roles, from Grade 7 up to SCS3.

Both GCO and EE terms

- Development of suggested options for reform

Out of Scope:

- Implementation of reforms (to be subject to later procurement).
- Salary survey benchmark pay data (we already source this data).

6. THE REQUIREMENT

6.1 The supplier will design and deliver a discovery programme to:

- Fully compare GCO's reward models, policies and policy outcomes with those of commercial/ procurement roles/teams in the external market
- Assess external competitiveness of pay and reward for commercial/procurement roles/teams, specifically:
- Base Pay Structures, including banding, ranges, progression, annual cycles
- Variable Pay (short-term Incentives / bonuses), including eligibility, design, metrics - Long-Term Incentives (LTIPs, or other deferred bonus arrangements) including eligibility, design, metrics
- Allowances, including type (location-based, role-specific, skills-based) treatment, eligibility
- Benefits and Perks, including health and wellbeing, leave, flexibility, access
- Pension provision, including employer contributions
- Pay Equity and Transparency
- Communications
- Governance and Policy Frameworks, including, oversight, approvals, stakeholders

6.2 Engagement activities, including surveys and focus groups, should ensure that a representative number of employees from both sets of T&Cs, and from all grades and departments are included.

6.3 Deliverables include:

1. Research report comparing the GCO reward framework with that in place in the private sector
2. Costed options for reform to the current reward framework
3. Proposed governance and accountability framework
4. Communications and change guidance
5. Proposed implementation plan

7. KEY MILESTONES AND DELIVERABLES

7.1 Milestones and timelines are subject to confirmation upon contract award, however, the following contract milestones/deliverables could apply:

Milestone/Deliverable Description	Timeframe or Delivery Date
1 External Data Gathering and Insights	4-6 weeks from contract commencement
2 Interim Findings Report	6-8 weeks from contract commencement
3 Final Reports, Plans and Guidance	8-12 weeks from contract commencement.

.

8. MANAGEMENT INFORMATION/ REPORTING

8.1 The Supplier will provide monthly written progress updates and quarterly presentations to the GCO Reward Project Board. Reports must include findings to date, risks, mitigations, and budget status.

9. VOLUMES

9.1 This review will cover approximately 875 GCO employees under GCO terms and 800 under Civil Service Equivalent terms. Engagement activities (surveys, focus groups) should ensure representative coverage across grades and departments. This is to assist the potential suppliers in assessing the requirement and their capability to meet it throughout the Contract duration.

10. CONTINUOUS IMPROVEMENT

10.1 The Supplier will be expected to apply continuous improvement throughout delivery, for example, improving data analysis, and incorporating emerging findings into draft outputs. Improvements will be discussed and agreed at contract review meetings.

10.2 Where relevant, the Supplier should present new ways of working to the Buyer during quarterly presentations to GCO Reward Project Board .

10.3 Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

11. SUSTAINABILITY / SOCIAL VALUE

Not applicable

12. QUALITY

12.1 Outputs must be in line with industry best practice, with clear evidence bases and transparent methodologies. Any benchmarking must cite reputable data sources (e.g., CIPS, Hays, HR Data Hub). Final outputs must be peer-reviewed and quality assured before submission.

13. PRICE

13.1 Suppliers should provide a fixed price for delivery of the discovery phase, broken down by activity (research, data analysis, benchmarking, reporting). All expenses must be included in the fixed price.

14. STAFF AND CUSTOMER SERVICE

14.1 The Supplier must provide sufficient qualified staff for the contract duration. Staff should have experience in reward design, Civil Service pay frameworks, benchmarking, and employee engagement research. Key staff should demonstrate experience of working with senior government stakeholders and commercial professions.

14.2 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

14.3 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

14.4 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

15. SERVICE LEVELS AND PERFORMANCE

15.1 The Buyer will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA description	Target
1	Engagement Coverage	Supplier must return a response rate of 80% across all engagement activities with GCO staff (GCO terms and Civil Service Equivalent Terms)	60% would constitute KPI Failure
2	Satisfaction on deliverables	Supplier must achieve a target of 95% satisfaction rating on the overall deliverables when reviewed	. 80% would constitute KPI failure
These criteria will be developed in conjunction with the Supplier.			

15.1 The Buyer will measure the quality of the Supplier's delivery by: KPI 1: Engagement Strategy Implementation
Description: The Supplier must design and implement a comprehensive engagement strategy to achieve a target response rate of 80% across all engagement activities with GCO staff (GCO terms and Civil Service Equivalent Terms).

The Supplier's obligation is to:
- Design an accessible, inclusive engagement strategy
- Deploy multiple engagement channels (surveys, focus groups, interviews)
- Implement targeted reminders and manager-led communications
- Monitor participation rates and deploy booster activities for

under-represented groups
- Report weekly on participation rates and actions taken

Target: 80% response rate
Measurement: The Supplier will be deemed to have met this KPI if it has implemented the agreed engagement strategy and can demonstrate reasonable endeavours to achieve the target, regardless of the actual response rate achieved.

Consequence of failure: If the 80% target is not achieved despite the Supplier's reasonable endeavours, the parties will jointly agree whether to accept the achieved response rate as representative or to extend the engagement period (using the optional 1-month extension) to conduct additional engagement activities.

KPI 2: Deliverable Quality and Satisfaction
Description: The Supplier must deliver high-quality outputs that meet the requirements set out in Section 6 of the Statement of Requirement.

Target: 95% satisfaction rating from the GCO Reward Project Board
Measurement: Within 10 Working Days of final delivery, the GCO Reward Project Board will complete a written satisfaction survey using a 5 point scale (1=very dissatisfied, 5=very satisfied). A score of 4.75/5 or above constitutes 95% satisfaction.

Consequence of failure: If the 95% target is not met, the Supplier will be given 10 Working Days to address the specific concerns raised by the Project Board and resubmit the deliverables for re-assessment. Payment will not be withheld provided the Supplier is making reasonable efforts to address the concerns.

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

16.1 All staff must hold baseline personnel security standard (BPSS) clearance as a minimum. Suppliers handling sensitive HR data must demonstrate compliance with GDPR, HMG security policies, and secure data transfer protocols.

17. PAYMENT AND INVOICING

17.1 Invoices will be submitted monthly aligned to deliverables and milestones outlined in , Section 7 of the Statement of Requirements , subject to satisfactory delivery of outputs. All invoices must include a breakdown of activities and deliverables completed.
17.2 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

18. CONTRACT MANAGEMENT

18.1 Contract Management will be facilitated via weekly check-in calls initially. To be determined. Attendance at any meetings shall be at the Supplier's own expense.

19. LOCATION

19.1 The services will be carried out primarily remotely, with occasional on-site workshops or presentations in London (Cabinet Office locations).

Annex 2: The Supplier's proposal
REDACTED TEXT under FOIA Section 43 (2), Commercial Information

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):

"EU GDPR"	the General Data Protection Regulation ((EU) 2016/679);
"Joint Control"	where two or more Controllers jointly determine the purposes and means of Processing;
"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 or further provided in writing by the Controller and may not be determined by the Processor.

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*) or as further provided in writing by the Controller, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against Personal Data Breach, 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. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take 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;

(iv) cost of implementing any measures; and which shall be maintained in accordance with Data Protection Legislation and Good Industry Practice; (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*)) and the Controller's further written instructions;

(ii) it uses all reasonable endeavours 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 UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74 of the DPA 2018); or

(ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018, as well as any additional measures determined by the Controller;

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

(iv) the Processor complies with its obligations under 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

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

(e) where the Personal Data is subject to EU GDPR, 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 transfer is in accordance with Article 45 of the EU GDPR; or

(ii) the Processor has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the Controller which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the Controller;

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

(iv) the Processor complies with its obligations under the EU GDPR 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);

(v) 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

(f) 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 full 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 but not limited to promptly 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 the Controller 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 other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

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 non-mandatory guidance issued by the Information Commissioner's Office, any relevant Central Government Body and/or any other regulatory authority. 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 non-mandatory guidance issued by the Information Commissioner's Office, relevant Central Government Body and/or any other regulatory authority.

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.

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are: dpo@cabinetoffice.gov.uk

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: REDACTED TEXT under FOIA Section 40, Personal Information

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

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

Description	Details
Identity of Controller and Processor for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: The following scope of Personal Data will be processed by the Supplier (as Processor) on the instructions of the Controller: Subject Matter of Processing: A comprehensive review of the Government Commercial Organisation (GCO) reward framework.
Duration of the Processing	• Start Date: The confirmed Call-Off Contract start date. • End Date: 30 calendar days after final written acceptance of all deliverables by the Controller. • Retention: All Personal Data will be securely deleted from all Supplier systems (including backups) within 30 calendar days of the End Date. The Supplier will provide written confirmation of deletion to the Controller.
Nature and purposes of the Processing	• Nature: The Supplier will receive, store, analyse, and report on Personal Data relating to GCO employees. • Purpose: To enable the Supplier to: ◦ Understand the current distribution and operation of pay, benefits, and reward across the GCO workforce.

	◦ Identify internal pay equity issues, compression points, and misalignments. ◦ Benchmark GCO reward practices against external commercial/procurement roles. ◦ Gather representative employee feedback on the current framework via surveys, focus groups, and interviews. ◦ Develop evidence-based, costed reform options for the Controller's consideration.
Type of Personal Data	Employee Identification: Unique employee ID. Role Data: Job title, grade (G7 to SCS3), department/directorate, terms and conditions status (GCO or Civil Service Equivalent), length of service, employment status (full-time/part-time). Reward & Pay Data: Base salary, allowances (type and amount), Performance-Related Pay (PRP) awards, bonus payments, pension contributions. Performance Data: Historical performance ratings (for PRP analysis). Demographic Data (for equal pay analysis): Gender, ethnicity, disability status, age band. Engagement Data: Survey responses (including free-text comments), focus group feedback, interview notes. De-identification of qualitative data. Survey free text, focus group notes and interview notes will be pseudonymised or summarised before analysis. No audio or verbatim transcripts will be retained by the Processor. Data minimisation. Performance ratings will be limited to the last three years unless otherwise instructed in writing by the Controller

Categories of Data Subject	• Approximately 1,675 GCO employees (875 on GCO terms, 800 on Civil Service Equivalent terms) at grades 7 to SCS3, employed across all government departments served by GCO. Special category data WILL be processed for the purposes of equal pay analysis and ensuring the reformed reward framework is fair and non-discriminatory. • Type of Special Category Data: Ethnicity, gender, disability status. • Lawful Basis for Processing: UK GDPR Article 9(2)(g) (processing necessary for reasons of substantial public interest) in conjunction with Schedule 1, Part 2, Paragraph 8 of the Data Protection Act 2018 (equality of opportunity or treatment).
	• Justification: The processing is necessary to identify and address potential pay inequalities, ensure compliance with the Public Sector Equality Duty, and support the development of a fair and transparent reward framework. • Appropriate Policy Document. The Controller confirms an Appropriate Policy Document under DPA 2018 Schedule 1 is in place for processing under Article 9(2)(g), and will share the APD reference with the Processor. The Processor will only process row-level special category fields for analysis within a pseudonymised workspace and will report aggregate outputs only, applying small cell suppression where n < 5 and excluding direct or indirect identifiers.
International transfers and legal gateway	All processing will take place within the United Kingdom. • Data will be stored on UK-hosted, encrypted cloud infrastructure. Microsoft 365 UK tenant for secure storage and collaboration and an agreed survey platform with UK data residency for staff surveys. Any change requires Controller approval and an updated Annex 1. • All Supplier personnel accessing the data will be UK-based. • No international transfers of Personal Data will occur.

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	All Personal Data will be securely deleted from all Supplier systems within 30 calendar days of the End Date. The Supplier will provide written confirmation of deletion to the Controller. Backups. Primary copies deleted within 30 days of the End Date. Immutable or offline backups overwritten on the next cycle and deleted within 90 days maximum. A deletion certificate will be provided."

Annex 2 - Joint Controller Agreement – NOT USED

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 [Supplier/Relevant Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours 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 [Supplier's/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

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

(a) report to the other Party every 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) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). 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) use all reasonable endeavours 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.

(k) Where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the nontransferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the nontransferring Party which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the
European Commission's SCCs (the **Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;

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

(iv) the transferring Party 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 non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

(l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of the nontransferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the EU GDPR; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures;

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

(iv) the transferring Party complies with its obligations under EU GDPR 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 non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

1.1.2.2 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

1.1.3.1 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 using such reasonable endeavours 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.

1.1.3.2 Each Party shall use all reasonable endeavours to restore, reconstitute 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

1.1.4.1 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.

1.1.4.2 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

1.1.5.1 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 non-mandatory guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. 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, any relevant Central Government Body and/or any other regulatory authority.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

1.1.7.1 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 to such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

1.1.7.2 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.

1.1.7.3 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.

1.1.7.4 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

1.1.9.1 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 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.