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

Order Form

CALL-OFF REFERENCE:	GSS24825
THE BUYER:	UK Research and Innovation (UKRI) (PS18244)
BUYER ADDRESS	Polaris House, North Star Avenue, Swindon, SN2 1FL
THE SUPPLIER:	Berkeley Square IT Ltd
SUPPLIER ADDRESS:	470 Bath Road, Bristol, BS4 3AP.
REGISTRATION NUMBER:	05195936
DUNS NUMBER:	739-432-131
SID4GOV ID:	N/A

This Order Form, when completed and executed by both Parties, forms a Call-Off Contract. A Call-Off Contract can be completed and executed using an equivalent document or electronic purchase order system.

If an electronic purchasing system is used instead of signing as a hard-copy, text below must be copied into the electronic order form **starting from 'APPLICABLE FRAMEWORK CONTRACT' and up to, but not including, the Signature block.**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated **07/11/2024**.

It's issued under the Framework Contract with the reference number RM6277 for the provision of Non Clinical Staff.

CALL-OFF LOT(S):

LOT 3

CALL-OFF INCORPORATED TERMS

This is a Bronze Contract.

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.
2. Joint Schedule 1 (Definitions and Interpretation) RM6277
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6277
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 7 (Financial Difficulties including Annex 5 Optional Terms for Bronze Contracts)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

    - Call-Off Schedules for RM6277
        - Call-Off Schedule 1 (Transparency Reports)
        - Call-Off Schedule 2 (Staff Transfer)
        - Call-Off Schedule 3 (Continuous Improvement)

4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6277

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 START DATE: **18/11/2024**

CALL-OFF EXPIRY DATE: **31/03/2025**

CALL-OFF DELIVERABLES

The provision of Non-Clinical Temporary staff

ASSIGNMENT:	Temporary Assignment
NUMBER OF ROLES REQUIRED:	1
JOB ROLE/TITLE:	Digital Business Analyst – [redacted]
AGENDA FOR CHANGE PAY BAND: (use rate card to determine this)	E

FEE TYPE:	Fee Type 2: Non-Patient Facing (Disclosure required)
DBS REQUIRED (FEE TYPE 1 AND 2 ONLY)	Basic
TEMPORARY WORK-SEEKERS COMPLIANCE REQUIREMENTS) State any other required clearance and/or background checking	Temporary Work-Seekers in Central Government will be checked to Baseline Personnel Security Standard plus any additional checks detailed below. None
PHOTO ID BADGE	For the avoidance of doubt the Photo ID Badge in compliance with Framework Schedule 1 (Specification) Clause 7.26 shall be provided by the Contracting Authority.
ENGAGEMENT OF TEMPORARY WORK-SEEKER	For the avoidance of doubt Joint Schedule 1 (Definitions) Clause 1.4 "Temporary Work-Seeker" shall apply "b) Any worker supplied to a Contracting Authority under this Framework Contract on a temporary basis, by a Supplier acting as an Employment Business, being a person who carries on business of their own account, through a limited company or otherwise and who works under supervision and direction of the Contracting Authority". Notwithstanding anything under this Agreement to the contrary, the manner in which a Temporary Work-Seeker engaged by the Supplier under a contract for services via a personal service company ("PSC"), provides the services during the Assignment, shall not be under or subject to the supervision, direction or control of the Contracting Authority or Supplier. For the avoidance of doubt, the Contracting Authority shall remain responsible for the PSC whilst on Assignment.

GDPR POSITION
Independent Controller

The Parties acknowledge that for the purposes of the Data Protection Legislation, under these Call Off Terms the Parties are independent Data Controllers of Personal Data. For the avoidance of doubt, Joint Schedule 11 Clauses 3 – 17 shall not apply.

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

CALL-OFF CHARGES
Charges as per the Framework Agreement. Discounts under Framework Schedule 1 Clause 13.24 and 13.25 will only be discounted to standard Framework Agreement Charges.

	AWR Compliant
Pay to Worker	[redacted] ex VAT.
Total Charge	[redacted] ex VAT.
The total contract value shall not exceed £57,196.86 excluding VAT as per the breakdown below: [redacted] Working Days @ [redacted] ex VAT = £57,196.86 ex VAT It is the viewpoint of the Contracting Authority that the job role above is in scope of the intermediaries legislation (IR35). All workers are subject to 14 working days' notice period.	

For the avoidance of doubt, the Supplier shall be entitled to increase the rates charged to the Contracting Authority at any time including, but not limited to, statutory changes bought about as a result of the Agency Workers Regulations 2010, Pension, Apprentice Levy and changes to the Working Time Directive and National Insurance contributions.

The Parties agree that for the fulfilment of Framework Schedule 1 (Specification) Clause 12.2 it is sufficient where the Supplier will show the Charges and hours worked on each invoice issued.

PAYMENT METHOD

Approval of a timesheet by the Contracting Authority will constitute acceptance Electronic Invoices will be issued weekly in arrears and the Contracting Authority shall pay the supplier within thirty (30) calendar days upon receipt and acceptance of a valid invoice. Invoice to include purchase order number and contract reference.

For the avoidance of doubt the Parties agree that Core Terms Clause 4.11 does not prevent the Supplier from raising genuine queries in relation to invoices or from working with CCS or the Contracting Authority to resolve invoicing issues.

The Contracting Authority confirms that the pay to the Temporary Worker will reflect the comparator rate under AWR and full holiday entitlement from day 1 of the assignment of 40.5 days including bank holidays.

BUYER'S INVOICE ADDRESS:
finance@uksbs.co.uk

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]
UK Shared Business Services Limited
Polaris House, North Star Avenue,
Swindon, SN2 1FL

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]
Berkeley Square IT, HERE Building, Bath Road,
Bristol, BS4 3AP

SUPPLIER'S CONTRACT MANAGER
[redacted]
Berkeley Square IT, HERE Building, Bath Road,
Bristol, BS4 3AP

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:		Name:	
Role:		Role:	
Date:		Date:	

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 UK 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 UK GDPR (or section 73 of 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, 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 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 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 determined by the non-transferring Party;

(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

(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 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: dataprotection@ukri.org.uk

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

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**The 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: • Personal Data held in relation to the performance of Temporary Worker compliance checks as detailed in paragraph 6 of Framework Schedule 1 (Specification). **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,

	• The scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority
Duration of the Processing	Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract. The Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data. The Authority may request access to Personal Data relating to performance of Temporary Worker compliance checks as detailed in paragraph 6 of Framework Schedule 1 (Specification) up to one (1) year after the end of an Assignment in order to perform its duties under paragraph 20 of Framework Schedule 1 (Specification).
Nature and purposes of the Processing	For all Assignments placed under the terms of the Framework Contract, Personal Data pertaining to the Temporary Worker will be collected, validated and retained by the Supplier in order to meet the Relevant Authorities specification with regards to the performance of Worker Compliance checks. For NHS Contracting Authorities such checks will be conducted in accordance with the NHS Employers Check Standards (see paragraph 6 of Framework Schedule 1). All Buyers have the right to request access to files containing Personal Data on Temporary Workers in order to assure that Temporary Worker compliance checks are conducted in accordance with their local policy and Framework Schedule 1 (Specification). The Authority may request, under the terms of this Framework Contract, access to files containing Personal Data on Temporary

	Workers deployed to Buyers in the NHS in order to perform its duties in providing a Temporary Worker compliance Audit function (see paragraph 20 of Framework Schedule 1). This may be conducted by a third party nominated by the Authority and provisions for processing Personal Data by the third party are to be no less onerous than those outlined in this Framework Contract. This Processing is required under the Conduct of Employment Agencies and Employment Businesses Regulations 2003 and NHS England policy relating to vetting of all workers. The Parties may retain business contacts for Supplier and Authority personnel for the purposes of the routine management of the Framework Contract.
Type of Personal Data	Personal Data to be processed in relation to the performance of Temporary Worker compliance checks as detailed in paragraph 6 of Framework Schedule 1 (Specification) shall include: • Identity checks • Right to work checks • Criminal record checks • professional registration checks • employment history and reference checks • workers health assessments • English language competency • statutory and mandatory training • appraisals and revalidation • umbrella company information This could include Processing of the following Personal Data - please note this list is not exhaustive: • Temporary Worker name and surname • Temporary Worker home address • Temporary Worker email address

	• Copies of Temporary Worker ID documents such as Passport, driving licence, ID card • Temporary Worker location data • Temporary Worker race or ethnic origin • Temporary Worker genetic data, biometric, data concerning health • Temporary Worker criminal history • Temporary Worker professional qualifications Other Processing for the purposes of routine framework management may require Processing of the following types of Personal Data: • Customer contact details including email addresses and phone numbers • Supplier contact details including email addresses and phone numbers
Categories of Data Subject	Categories of Data Subject include: • Temporary Workers • Supplier staff • Buyer staff
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 shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract. The Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data. The Parties will have and maintain privacy policies for the management of Personal Data under the applicable Data Protection Legislation and, plans for destruction of data once the Processing is complete. The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained, and to destroy any physical copies of Personal Data, 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.