



## DPS Schedule 6 (Order Form Template and Order Schedules)

### Order Form

ORDER REFERENCE: LRSR246 / C200896 / C229128

THE BUYER: UK Health Security Agency

BUYER ADDRESS 10 South Colonnade, London, E14 5EA

THE SUPPLIER: Ipsos (Market Research) Limited

SUPPLIER ADDRESS: 3 Thomas More Square  
London, E1W 1YW, UK

REGISTRATION NUMBER: 948470

DUNS NUMBER: 227257185

DPS SUPPLIER REGISTRATION SERVICE ID: SQ-ABE7ZEU

START DATE: 30<sup>th</sup> January 2024, or the date on which the last party signs

INITIAL TERM: Two Years

MAX TERM: Three Years

MAX VALUE: £1,900,000.00

#### SERVICES:

Quantitative market research via ad hoc projects and public perceptions tracking to provide robust insight into knowledge, attitudes, and behaviours of the public and groups within the population in relation to specific public health hazards, informing the preparedness and response work of teams across UKHSA.



## APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 30<sup>th</sup> January 2024. It's issued under the DPS Contract with the reference number LSRS246 / C200896 / C229128 for the provision of Quantitative Research – Ad hoc & Public Perception Tracking.

## DPS FILTER CATEGORIES:

Conjoint / discrete choice / MAXDIFF / stated preference / trade-off, Segmentation analysis, Quantitative, CAPI (computer assisted personal interview), CATI (computer assisted telephone interview), Omnibus, Behaviour change, Tracking research, Public polling, England, Wales, Scotland, Northern Ireland

## ORDER INCORPORATED TERMS

The following documents are incorporated into this Order 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 Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6126 Research & Insights
3. Not used
4. The following Schedules in equal order of precedence:
  - Joint Schedules for RM6126 Research & Insights LSRS246 / C200896 / C229128
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 6 (Key Subcontractors)
    - Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)
    - Order Schedules for RM6126 Research & Insights LSRS246 / C200896 / C229128
    - Order Schedule 1 (Transparency Reports)
    - Order Schedule 2 (Staff Transfer)
    - Order Schedule 3 (Continuous Improvement)
    - Order Schedule 4 (Order Tender)
    - Order Schedule 5 (Pricing Details)
    - Order Schedule 9 (Security) Part A
    - Order Schedule 20 (Order Specification)
5. CCS Core Terms (DPS version) v1.0.3
6. Joint Schedule 5 (Corporate Social Responsibility) DPS RM6126 LSRS246/C200896/ C229128



No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

Call offs made against this contract for Quantitative Market Research (Ad hoc) will be issued via a Letter of Appointment following the numbering format: LSRS246.01, LSRS246.02 etc. Payment method detailed below.

For the delivery of Public Perception Tracking against this contract each wave of tracking will be signed off by the contract Manager (Clare Deahl or the secondary contact given below) in good time prior to the next wave of tracking. Payment method detailed below.

#### ORDER SPECIAL TERMS

The parties agree that 30 days prior the date on which the Supplier is required to share its Confidential Information, the Buyer and Supplier shall meet and agree in good faith the information that should reasonably be included in the disclosure, specifically taking into account information which is strictly necessary for the delivery of the Replacement Services. The Buyer shall not permit the actual or prospective Replacement Supplier to use the Supplier Confidential Information, for any reason other than for the delivery of the Replacement Services.

ORDER START DATE: 30<sup>th</sup> January 2024

ORDER EXPIRY DATE: 29<sup>th</sup> January 2026

ORDER INITIAL PERIOD: Two Years

#### DELIVERABLES

See details in Statement of Requirements, as issued in Tender Pack dated 19 October 2023.

#### MAXIMUM LIABILITY

The limitation of liability for this Order 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 £949,999.99

#### ORDER CHARGES

See Pricing Details in Price Schedule as per Tender submission dated 13<sup>th</sup> November 2023.

#### REIMBURSABLE EXPENSES

None

**PAYMENT METHOD**

All invoices must be sent, quoting a valid purchase order number (PO Number) to:

[REDACTED]

**Ad Hoc Projects**

Each commission will be covered by a PO, which will be issued within 20 days of a countersigned LoA

You must be in receipt of a valid PO Number before submitting an invoice.

**Public Perception Tracker**

Within 20 Working Days of countersignature of this Order Form, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.

To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Buyer contact (i.e., Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment.

If you have a query regarding an outstanding payment, please contact our Accounts Payable section by email to:

[REDACTED]

**BUYER'S INVOICE ADDRESS:**

Accounts Payable

10 South Colonnade, London, E14 5EA

**BUYER'S AUTHORISED REPRESENTATIVE**

[REDACTED]

**Secondary Contact:**

[REDACTED]

For Commercial liaison your contact will be:

[REDACTED]

**BUYER'S ENVIRONMENTAL POLICY**

Corporate report: Environmental Policy Published 7 November 2022 available online at:  
Environmental policy - GOV.UK ([www.gov.uk](http://www.gov.uk))

**BUYER'S SECURITY POLICY**

DHSC Data Protection Policy:



DHSC Data  
protection policy.pdf

**SUPPLIER'S AUTHORISED REPRESENTATIVE**

3 Thomas More Square, London, E1W 1YW

**SUPPLIER'S CONTRACT MANAGER**

1YW

**PROGRESS REPORT FREQUENCY**

For each project upon commissioning (including on-going public perceptions tracking), a detailed timeline with key milestones will be agreed between the Buyer and Supplier.

A weekly status update for each project (a short virtual meeting or email update, depending on need). Where multiple projects are being delivered at the same time this can be combined into one status update covering all projects.

The supplier shall take no more than 24 hours to respond to contract and project queries from UKHSA within the standard working week (Monday to Friday), allowing additional time for public holidays.

**PROGRESS MEETING FREQUENCY**

A monthly project management meeting to review in detail the delivery of current projects (e.g., progress towards meeting agreed deadlines and producing deliverables, early identification of risks to delivery and mitigating actions), and to discuss potential future requirements.

A formal quarterly contract management meeting to review performance against the contract management plan and deliverables as detailed in Statement of Requirements.



Meeting schedule to be confirmed between buyer and supplier upon commencement of contract.

#### KEY STAFF

The supplier will provide a named member of staff of sufficient seniority who will be the key day-to-day contact.



3 Thomas More Square, London, E1W 1YW

#### KEY SUBCONTRACTOR(S)

Rackspace UK

#### E-AUCTIONS

Not applicable

#### COMMERCIALLY SENSITIVE INFORMATION

Not applicable

#### SERVICE CREDITS

Not applicable

#### ADDITIONAL INSURANCES

Not applicable

#### GUARANTEE

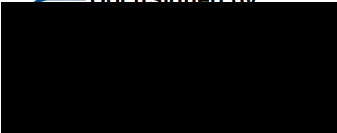


Not applicable

#### SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)



Signed:

For and behalf of the Supplier:	For and behalf of the Buyer:
<div>DocuSigned by: </div> <div>Full Name: </div> <div>Job Title/Role: </div> <div>Date Signed: 31/01/2024</div>	<div>DocuSigned by: </div> <div>Full Name: </div> <div>Job Title/Role: </div> <div>Date Signed: 31 Jan 2024</div>

## 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*);
      - (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 Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
    - (ii) the Data Subject has enforceable rights and effective legal remedies;
    - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
    - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
  - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
7. Subject to paragraph 7 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 6 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 6 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 8 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*).



UK Health  
Security  
Agency

RM6126 DPS Order Form  
Quantitative Research – Ad hoc & Public Perception Tracking

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 27 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 agreed by both parties.

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

## Annex 1A: Schedule of processing

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Parties are Joint Controllers</b></p> <p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of the research responses. The Supplier is the sole Controller of the research participant sample.</p> <p>Research participants in scope of this contract are members of the general public and health and social care workers or other professionals or volunteers working in roles or for organisations which may have a public health related remit, for example, teachers.</p> <p>Personal Data will be collected by the Supplier to identify people to take part in quantitative research, as determined by the requirements of individual projects commissioned under this call off contract. Personal Data collected will include: age, gender, region, ethnicity, religion, disability or health condition, income, work status, job role, post code, number and age of children in household, unpaid caring responsibilities, sexual orientation, pregnancy.</p> <p>All participation in quantitative research delivered under this call-off contract will be anonymised by the Supplier prior to sharing the responses with the Relevant Authority.</p>



<p>Duration of the Processing</p>	<p>The processing will take place over duration of the contract (2 years) and potentially up to one year of extension.</p> <p>For each individual project commissioned via the call-off contract, the Supplier will retain Personal Data relating to the project for as long as is reasonable to deliver the work. Upon project completion, the Supplier will delete all personal data relating to the project and when requested in writing, provide the Relevant Authority with proof of disposal within six months of completion. Notwithstanding the foregoing, the Supplier will retain one copy of confidential information in its archives for routine backup purposes only, this does not include personal data and the obligations of confidentiality relating to such retained materials shall continue for as long as such materials are retained.</p>
<p>Nature and purposes of the Processing</p>	<p>Personal Data will be processed by the Supplier in order to effectively conduct ad-hoc quantitative and public perceptions tracking research. The Supplier will not share any identifiable Personal Data with UKHSA.</p> <p>This call-off contract will require the Supplier to process Personal Data for the purposes of:</p> <ul style="list-style-type: none"> <li>a) sampling - to ensure that those participating in research meet the criteria needed to fulfil the requirements of the research brief</li> <li>b) data analysis - to enable the Supplier to analyse the relationship between different variables, such as age, gender, health status, within the data set</li> </ul> <p>Personal Data will be stored securely by the Supplier, complying with GDPR and relevant ISO standards.</p> <p>The Supplier will destroy all Personal Data within six months after the final research output has been delivered for each project commissioned through the contract (with the exception of the archiving copy agreed above). The Supplier will only retain final versions of Deliverables shared with the Relevant Authority, for the purpose of building a knowledge bank to add value to UKHSA over the call-off contract lifecycle, as well as final versions of research instruments for the purpose of swiftly setting up new research projects that build on previous learning.</p>



Type of Personal Data	<p>All or some of the following data may be collected by the Supplier, depending on the individual project need.</p> <p>Any contact details (telephone number or email address) that are collected by the Supplier will never be shared with UKHSA. All other Personal Data will be aggregated and anonymised before sharing with UKHSA.</p> <ul style="list-style-type: none"> <li>• Telephone number</li> <li>• Post code</li> <li>• Email address</li> <li>• Age</li> <li>• Gender identity</li> <li>• Region</li> <li>• Ethnicity</li> <li>• Religion</li> <li>• Disability</li> <li>• Health condition</li> <li>• Income</li> <li>• Work status</li> <li>• Job role</li> <li>• Number and age of children in household</li> <li>• Unpaid caring responsibilities</li> <li>• Sexual orientation</li> <li>• Pregnancy</li> </ul>
Categories of Data Subject	<p>Research participants in scope of this contract are members of the general public and health and social care workers or other professionals working roles or organisations which may have a public health related remit, for example, teachers</p>



Plan for return and destruction of the data once the Processing is complete  UNLESS requirement under Union or Member State law to preserve that type of data	The Supplier will destroy all Personal Data within six months after the final research output has been delivered for each project commissioned through the contract (with the exception of the archiving copy agreed above. This does not contain Personal Data). They will only retain final versions of Deliverables shared with the Relevant Authority, for the purpose of building a knowledge bank to add value to UKHSA over the call-off contract lifecycle.
---	---

## Annex 1B: Security

Added in accordance with PPN 03/22: [PPN 03/22 – Updated guidance on data protection legislation - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/ppn-0322-updated-guidance-on-data-protection-legislation) This supplements Schedule 9 which relates to general security requirements.(Corrinne Oldknow UKHSA Legal)

**External Certifications** The Supplier shall hold at least Cyber Essentials Plus certification (or an equivalent) and ISO 27001:2013 certification.

**Risk Assessment** The Supplier shall perform a technical information risk assessment on the Services supplied and be able to demonstrate what controls are in place to address those risks.

**Security Classification of Information** The Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that information classified as OFFICIAL, OFFICIAL-SENSITIVE and/or Personal Data is safeguarded in accordance with the applicable legislative and regulatory obligations.

## End User Devices

The Supplier shall ensure that any Buyer Personal Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer except where the Buyer has given its prior written consent to an alternative arrangement.

The Supplier shall ensure that any device which is used to Process Buyer Personal Data meets all of the security requirements set out in the NCSC End User Devices

Platform Security Guidance, a copy of which can be found at:  
<https://www.ncsc.gov.uk/guidance/end-user-device-security>

**Testing** The Supplier shall at its own cost and expense, procure a CHECK or CREST Certified Supplier to perform an ITHC or Penetration Test prior to any live Buyer Personal Data being transferred into its systems. The ITHC scope must be agreed with the Buyer to ensure it covers all the relevant parts of the system that processes, stores or hosts Buyer Personal Data.

**Networking** The Supplier shall ensure that any Buyer Personal Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

**Personnel Security** All Processor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Deliverables. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Supplier may be required to implement additional security vetting for some roles.

**Identity, Authentication and Access Control** The Supplier must operate an appropriate access control regime to ensure that users and administrators of the Deliverables are uniquely identified. The Supplier must retain records of access to the physical sites and to the Deliverables.

**Data Destruction/Deletion** The Supplier must be able to demonstrate it can supply a copy of all Buyer Personal Data on request or at termination or expiry of the Contract, and must be able to securely erase or destroy all data and media that the Buyer Personal Data has been stored and processed on.

**Audit and Protective Monitoring** The Supplier shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Buyer Personal Data. The retention periods for audit records and event logs must be agreed with the Buyer and documented.

**Vulnerabilities and Corrective Action** The Supplier shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

The Supplier must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Supplier COTS Software and Third Party COTS Software are always in mainstream support.

**Secure Architecture** The Supplier shall design the service in accordance with:

- NCSC "[Secure design principles - NCSC.GOV.UK](#)"
- NCSC "[Protecting bulk personal data - NCSC.GOV.UK](#)"
- NSCS "[The cloud security principles - NCSC.GOV.UK](#)"

## Annex 2 - Joint Controller Agreement

### 1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 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, where applicable, agree that the Supplier:

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is responsible for the Parties' compliance with all reasonable 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

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

- (a) report to the other Party every 3 months on:
  - (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
  - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
  - (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
  - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
  - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

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

- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
  - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
  - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
  - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
- (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Personal Data Breach;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

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

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

### 3. **Data Protection Breach**

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

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
  - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
  - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
  - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
  - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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



- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

#### 4. **Audit**

##### 4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

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

#### 5. **Impact Assessments**

##### 5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.



## 6. ICO Guidance

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

## 7. Liabilities for Data Protection Breach

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

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

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

Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):
- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
  - (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
  - (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.
- 7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

## 8. Termination

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

## 9. Sub-Processing

- 9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
  - (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

## 10. Data Retention



UK Health  
Security  
Agency

RM6126 DPS Order Form  
Quantitative Research – Ad hoc & Public Perception Tracking

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



### Order Schedule 4 (Order Tender)

Tender proposal submitted by Ipsos (Market Research) Limited in response to Technical Questions 4 – 9 dated 10<sup>th</sup> November 2023

## Quantitative research methods

#### 4.1 Quantitative research capabilities for ad-hoc research

[illegible]



[Redacted content]

[Redacted content]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]





[Redacted text block]

5.1 Robust and high-quality sampling of specific groups

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted content]



[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

5.2 Sampling approach for the public attitudes and behaviours tracker

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

- [Redacted list item 1]
- [Redacted list item 2]
- [Redacted list item 3]
- [Redacted list item 4]
- [Redacted list item 5]
- [Redacted list item 6]
- [Redacted list item 7]
- [Redacted list item 8]
- [Redacted list item 9]
- [Redacted list item 10]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



## 6. Data analysis and reporting

### 6.1 Quantitative analysis approaches

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted content]



6.2 Producing engaging and accessible outputs

[Redacted text block]

[Redacted text block]



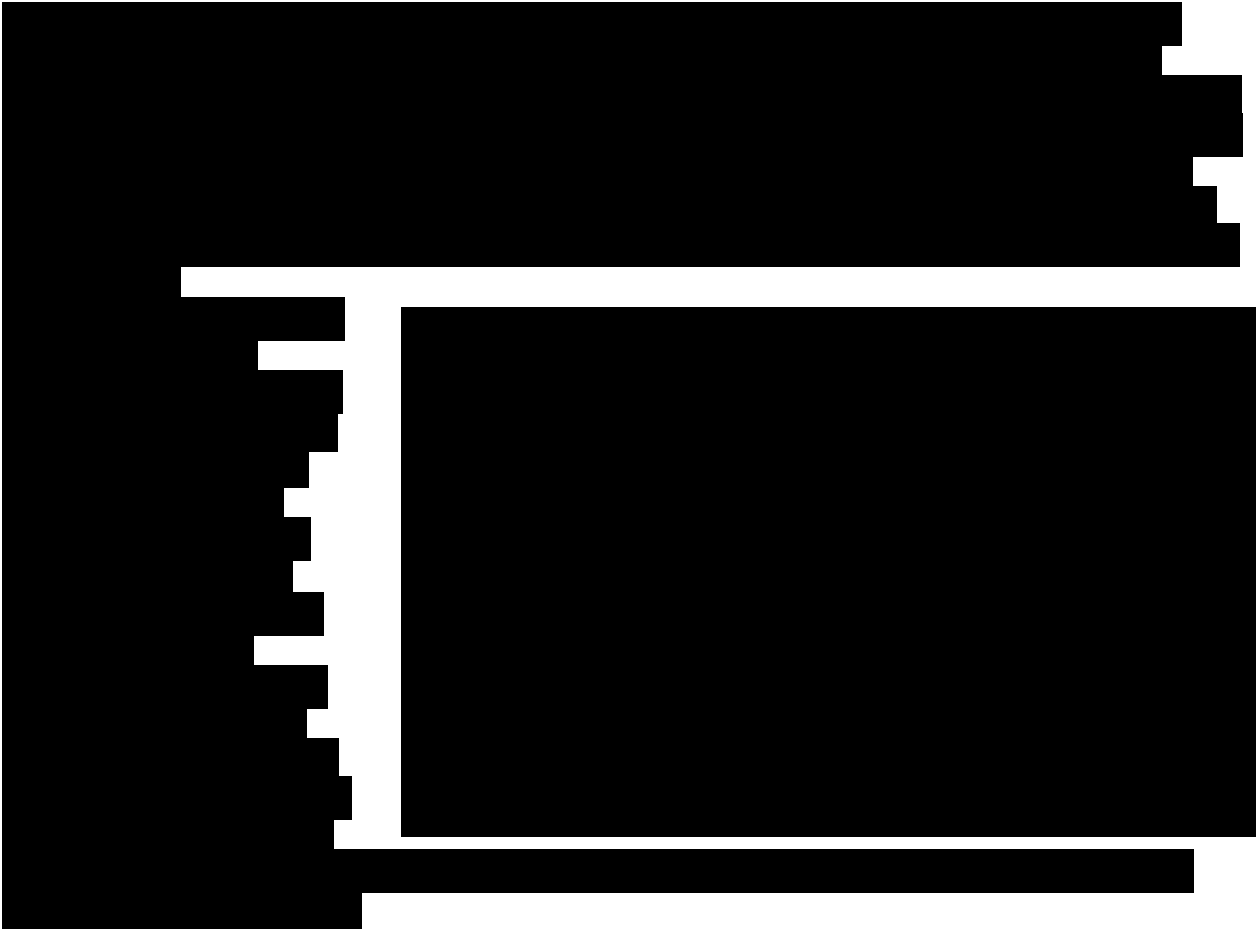
[Redacted text block]



[Redacted content]



[Redacted content]







7. Team and resourcing

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]



<div> <div></div> <div></div> </div>		<div> <div></div> <div></div> </div>	
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>		<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>		<div> <div></div> <div></div> </div>



[Redacted]		[Redacted]
[Redacted]		

7.2 Capacity to deliver

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



## 8.1 Quality assurance

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

\_\_\_\_\_

[illegible]



<div data-bbox="191 264 422 383" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="191 383 422 853" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="422 264 443 383" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 383 443 456" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 456 443 645" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 645 443 786" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="480 264 1461 383" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 383 1461 568" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 568 1461 710" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 710 1461 853" data-label="Text"><p>[Redacted]</p></div>
<div data-bbox="191 853 422 898" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="191 898 422 1550" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="422 853 443 898" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 898 443 1122" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 1122 443 1339" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="480 853 1461 1039" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 1039 1461 1263" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 1263 1461 1404" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 1404 1461 1550" data-label="Text"><p>[Redacted]</p></div>
<div data-bbox="191 1550 422 1637" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="191 1637 422 1998" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="422 1550 443 1594" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="422 1594 443 1890" data-label="Text"><p>[Redacted]</p></div>	<div data-bbox="480 1550 1461 1733" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 1733 1461 1874" data-label="Text"><p>[Redacted]</p></div> <div data-bbox="480 1874 1461 1998" data-label="Text"><p>[Redacted]</p></div>




[Redacted content]

9.1 Social value

[Redacted content]

[Redacted content]

[Redacted content]



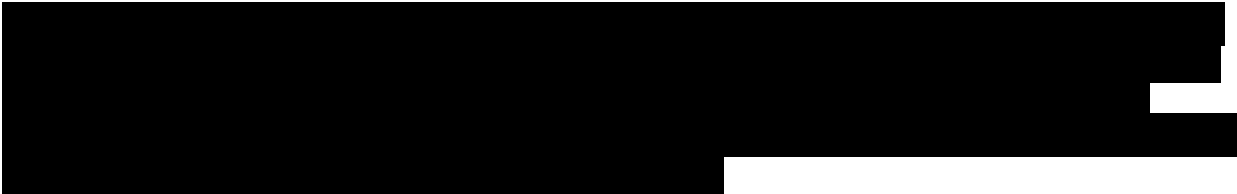



[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



your		

[Redacted content]





Order Schedule 5 (Pricing Details)

Day Rates

Submitted by Ipsos (Market Research) Limited as part of commercial evaluation to be used for future ad hoc projects dated 10<sup>th</sup> November 2023.

Job Level	Proposed worker (if known)	Example Activity	Daily Rate

