NOT TO BE USED WHERE RESPONDENT IDENTIFYING INFORMATION IS TO BE PROVIDED TO THE CLIENT

Supplier - Terms & Conditions of Contract

Reference is made to the proposal to which this document is attached , issued by Supplier to Client for the provision of market research services or other related services (the "**Services**") identified in the proposal or other similar document issued by Supplier relating thereto (the "**Proposal**"). The general terms and conditions below (the "**T&Cs**"), the Proposal and the description and other specifications of the Services identified in the Proposal shall be collectively referred to herein as the "**Agreement**".

DEFINITIONS AND INTERPRETATION

In these T&Cs, unless the context otherwise requires, the following definitions shall apply:

"Client" means the person or entity to which the Proposal for the Services has been issued by Supplier.

"Supplier" means the relevant Supplier entity referred to in the Proposal from time to time including but not limited to Market & Opinion Research International Limited, Ipsos MORI UK Limited and Ipsos Healthcare (Japan) Limited.

"Deliverables" means the presentations, reports, data or other results of the Services identified in the Proposal and specifically prepared by Supplier for the Client.

"Confidential Information" shall mean all information relating to the intellectual property and business practices of either party including, without limitation: (i) information relating to research and development, methodologies, processes, know-how, specifications; and (ii) business plans, financial information, products, services, costs, sources of supply, strategic, advertising and marketing plans, customer lists, pricing methods, project and commercial proposals (including the Proposal and the Proposal and any information contained in those documents), personnel, and business relationships.

CONTRACT

1. The Proposal issued to the Client by Supplier may be withdrawn or varied at any time and unless otherwise specified shall be automatically withdrawn after 30 days.
2. All work undertaken by Supplier is subject to these T&Cs unless otherwise agreed in writing. The Client acknowledges and agrees that no other document, in particular its own general conditions of purchase or specific conditions of sale, shall prevail over the T&Cs unless it has been expressly agreed by Supplier.
3. Any changes to the specifications or scope of the Agreement must be agreed in writing by the parties and may result in changes to the costs and timings proposed.

PRICE AND PAYMENT

4. The price of the Services shall be the fee quoted and confirmed in the Proposal. All fees quoted exclude Value Added Tax and/or any other required taxes or duties. Where applicable, government sales, withholding, use and/or value added taxes shall be paid by Client in addition to the fees due under this Agreement. Client shall in no event be liable for payment of any taxes based on Supplier's net income or personal property. If Client is required by law to make any deduction or withholding from any sum payable by it to or for the account of Supplier, the sum payable by Client in respect of which deduction or withholding is required to be made shall be increased to the extent necessary to ensure that, after the making of such deduction or withholding, Supplier receives and retains (free from liability in respect of such deduction or withholding) a net sum equal to the sum which it would have received and so retained had no such deduction or withholding been made.
5. Additional costs and expenses incurred by Supplier for the needs of the Services, including, out of pocket expenses such as transport and accommodation expenses, or third party pass through expenses which are not included in the price quoted or which could not be anticipated at the date of the Proposal, shall be reimbursed to Supplier by the Client. Claims for all such costs and expenses will be submitted to the Client with receipts.
6. Unless otherwise agreed in the Proposal, the fee of the Services will be invoiced in two parts. 70% will be invoiced when the Client commissions the Services and 30% (together with any costs and expenses incurred) will be invoiced on despatch or presentation of the Deliverables, whichever is the sooner, except for Services consisting of syndicated products, tracking surveys or other long term surveys, in which case Supplier will define different project phases in the Proposal and will invoice Client the full amount of the fees corresponding to each phase at the beginning of each such phase. Supplier also reserves the right to require the entire fee to be paid in advance.
7. Unless otherwise agreed in the Proposal, the fee is payable by the Client within 30 days of receipt of Supplier's invoice. All payments shall be made in full without deduction in respect of any set-off or counterclaim. If on expiry of 60 days any invoice remains unpaid Supplier will add a further surcharge of 2.5% for each month or part month during which the monies have not been received.
8. If the Client fails to make any payment thirty (30) days after the due date, then without prejudice to any other right or remedy available to Supplier, Supplier shall be entitled to:
   a. terminate the Agreement or, in the alternative, suspend any further services to the Client until such amounts have been paid;
   b. appropriate any payment made by the Client to such of the Services (or the research supplied under any other contract between the Client and Supplier) as Supplier may think fit;
9. Where the Agreement involves receipts or payments in foreign currency, Supplier shall have the right to increase the Services fee if on the due date of payment, the rate of exchange of the two currencies has changed so that the value of the currency specified in the invoice compared to sterling has increased by more than 1% from the date of the commission. The prevailing exchange rates shall be those specified by the Financial Times (or if published in any equivalent source) on the date of the Proposal and the payment date.
10. Supplier reserves the right by giving notice to the Client at any time before delivery, to increase the price of the Services (or any related out of pocket expenses) to reflect any increase in the cost to Supplier which is due but not limited to any factor beyond the control of Supplier, including, but not limited to any request by Client for a change in delivery dates, quantities, specifications or scope of the Services, any delay caused by instructions of the Client, failure of the Client to give Supplier accurate information or instructions, or any changes in the law.

EARLY TERMINATION OR POSTPONEMENT OF RESEARCH BY CLIENT:

11. In the event of Services being cancelled by the Client after commissioning but before commencement of fieldwork, Supplier will impose a cancellation charge of up to 25% of the total quoted fee, or the actual fees and expenses incurred by Supplier up to the effective date of termination, together with any unrecoverable third party costs incurred. In the event of cancellation after the commencement of fieldwork Supplier reserves the right to charge the full fee. If Client delays or postpones the Services, Client shall pay for any documented unrecoverable costs incurred by Supplier as a result of such delay or postponement.

CHANGE CONTROL

12. Should either party wish to change any aspect of the Services (including adding new services to the Services) it shall provide the other party with details of the proposed changes in writing (a "Change Request"). Within a reasonable period from receipt of the Change Request from the Client, and in the case of a Change Request by the Supplier, the Supplier shall inform the Client of:
    a. the impact of the proposed change upon the Services;
    b. the impact of the proposed change on the price of the Services; and
    c. any other terms herein that may be affected by the proposed change.
13. The other party shall not be obliged to agree a Change Request.

RESEARCH OBLIGATIONS

14. Supplier follows the requirements of the Market Services Society (MRS) Code of Conduct, the International Chamber of Commerce (ICC) and ESOMAR and the disclosure rules set by the British Polling Council (BPC) (where applicable), as amended by these T&Cs. In addition, Supplier is accredited to the quality standard ISO 20252, ISO 9001 and ISO 27001 details of which are available on request.
15. Whilst Supplier will use all reasonable endeavours to deliver the Services within the agreed timing, under no circumstances will it be responsible for any delays.
16. From time to time, Supplier may, where appropriate, subcontract work on the Services to one of its approved suppliers, subsidiaries or affiliates located in and outside the UK. Where requested, Supplier will inform the Client about the identity of its approved suppliers.
17. Where the sample is drawn from computerised lists of names and addresses supplied by the Client, the Client and Supplier warrant that they will comply with the requirements of the data processor clauses set out in Appendix 1 of these T&Cs.
18. Furthermore, in accordance with its professional rules and its contractual obligations to respondents, Supplier is under a duty to preserve the anonymity of the respondents when providing market, opinion and social research and data analytics services. Accordingly, Supplier shall only provide Client with aggregate data or otherwise anonymized data. Client hereby undertakes to respect this anonymity and undertakes not to attempt to link the data provided by Supplier to the identity of the respondents. Supplier will only provide Personal Data to Client as permitted by and in accordance with its professional rules and applicable Data Protection Legislation (as defined in Appendix 1). In any instance of such permitted disclosure, Client hereby agrees to maintain the confidentiality of such Personal Data. Where such Personal Data is provided by Supplier, acting as a Data Controller, to Client, Client warrants that it will cease further use or processing of the Personal Data upon notice from Supplier, and shall comply with all instructions included in such notice, including deletion of any or all relevant Personal Data.
19. Where a requirement is made to the Client under the Freedom of Information Act 2000 to access information from the Client which was obtained via Supplier, then the Client will (a) inform Supplier of full details of such request as soon as is reasonably possible, and (b) consult with and take into account the views of Supplier. Supplier reserves the right to pass onto the Client its reasonable and evidenced expenses incurred in connection with assisting the Client deal with information requests received under such legislation.

CONFIDENTIALITY

20. Neither party receiving Confidential Information from the other party shall
    (i) use Confidential Information received from the other party under this Agreement for any purpose other than to fulfil its obligations under this Agreement;

(ii) (ii) disclose such Confidential Information to any third party, except for those of its employees with a need to know the information in order to perform their obligations hereunder and provided that they are made aware of and agree to be bound by the obligations of confidentiality contained herein. The receiving party further agrees to use the same degree of care in safeguarding the confidential information as its uses for its own information, but in no event less than a reasonable degree of care. All Confidential Information in tangible form (including any copies or summaries of Confidential Information) shall be returned to the disclosing party promptly upon written request, upon termination of the Agreement or upon the receiving party's determination that it no longer has a need for such Confidential Information. Confidential Information provided to the receiving party in any other form, to the extent such information cannot be returned to the disclosing party, shall be destroyed by the receiving party to the extent practicable.

21. The obligation of confidentiality, however, shall not apply to information which: (i) is, at the time of receipt or dissemination, or thereafter becomes generally available to the public; (ii) the receiving party possessed at the time of receipt thereof from the disclosing party, and was not acquired directly or indirectly from the disclosing party; (iii) is acquired or rightfully received and without confidential limitation by the receiving party from a third party; (iv) is independently developed by the receiving party without breach of this Agreement; or (v) is required to be disclosed pursuant to court order or law requirement, provided that receiving party first gives the disclosing party reasonable notice of such court order or law requirement and an opportunity to oppose and/or attempt to limit such production.
22. Notwithstanding the foregoing, Client acknowledges and agrees that certain Services may require Supplier to expose, reveal, disclose or describe Client's confidential information, including, without limitation, new concepts, products, services, advertising campaigns or designs, to survey respondents ("Concept Testing"). Client hereby waives and releases Supplier from and against any and all Claims resulting from or related to Supplier's disclosure of Client's confidential information to survey respondents in connection with Concept Testing.

INTELLECTUAL PROPERTY RIGHTS

23. Client shall own the Deliverables (including copyright or other intellectual property rights) upon payment of the relevant price. Supplier retains full ownership and intellectual property rights in all techniques, models, processes, tools, methodologies and know-how, (including without limitation all databases, computer programs and software, processes, formulae, tools, models, algorithms and products, proposals survey questionnaires, data files and other forms used in the fieldwork) that are used, created or developed in connection with the Services ("Supplier IP").
24. Under no circumstances will Supplier disclose information regarding respondents that will make them personally identifiable except as permitted by and in accordance with applicable law and professional codes of conduct.
25. Notwithstanding the foregoing, to the extent that the Agreement specifies that the Services include normative data to assist the Client with the interpretation of the Services, syndicated research services and/or any Deliverables will be comprised of syndicated research reports ("Syndicated Deliverables"): (i) Supplier shall at all times retain sole and exclusive ownership rights in the Syndicated Deliverables as well as all Supplier IP; (ii) Client may not sell, distribute, copy or reproduce in full or in part any of the Syndicated Deliverables, without authorisation from Supplier, which Supplier may withhold in its sole discretion; and (iii) this Agreement constitutes a revocable, non-exclusive license from Supplier to Client to use the Syndicated Deliverables solely for internal purposes, subject at all times to the ownership rights of Supplier set forth herein.
26. Neither the Client nor Supplier shall have the right to use the other's trade marks without prior written consent, except for the purposes of Supplier's marketing purposes or promotional materials, including on Supplier's website.

USE OF DELIVERABLES

27. In order to enable the Supplier to comply with the requirements under the MRS and ESOMAR codes of conduct, the use of the Deliverables by the Client is limited as follows:
    a. If Client or its agents wish to publish the Deliverables in the public domain including, without limitation, in advertising, marketing or promotional materials, social media, press releases or press conferences, it must come to a written agreement with Supplier on the form and content of the disclosure, which Supplier may **only** withhold on the basis that the Deliverables are used or presented in a misleading or illegal manner, or in any manner which would adversely impact upon the reputation or goodwill of Supplier. Supplier reserves the right to publish a correction in the event of such improper use or presentation.
    b. The Client may only use the Deliverables in connection with any dispute resolution, litigation, arbitration or other legal proceeding of any nature ("Litigation Purposes") not initiated by it, unless the Litigation Purpose is directed against the Supplier. The Client confirms that it does not intend to use of the Deliverables for Litigation Purposes, as this may affect Supplier's recommended methodological approach and study costs set out in the Proposal. In addition, if the Client decides after the Services has been completed that it wishes to use the Deliverables for Litigation Purposes, it must first obtain with the prior written consent of Supplier, which Supplier may withhold in its sole discretion.
28. The Client must ensure that Supplier is credited for all published Services as "a poll/research conducted by Supplier for.....(Client)".
29. Once the data has been published, it is in the public domain and Supplier has the right to disseminate the results and technical details to other parties and to publish them.

OPINION POLLS

30. The following specific rules shall apply where the Services are an opinion poll:
31. Every report published by or on behalf of the Client, of the poll findings should give: for whom and by whom the sample survey was conducted, the purpose of the survey, the method, a definition of the population sampled, the size and nature of the sample, the number, type and geographical distribution of sampling points, the method by which the information was collected, the full question wording used, and dates of fieldwork and the bases of all percentages. Similar standards are applied to desk research based on published material.
32. Where data from a private poll is leaked to the media either by a Client or by a third party, Supplier reserves the right to clarify/correct any misleading or incorrect impressions and to provide the full results and technical details.
33. Where, in reply to questions on voting intention, there are abnormal levels or sharp changes in the manner of those who say they would not vote or who are undecided, these facts will be reported.
34. In accordance with the British Polling Council's Code of Conduct the results of the questions on voting intention of the general public will only be published if these results are based on a representative sample of 1,000 or more respondents.

INDEMNIFICATION

35. The Client shall indemnify and hold harmless Supplier, its employees, officers, directors and agents from and against any and all loss, claim or liability, including without limitation reasonable legal fees and costs, that may arise in connection with (i) the Client's disclosure of the Deliverables to any third party, (ii) the use of the Deliverables in the public domain by the Client or any third party to whom the Client has disclosed the Deliverables, (iii) the use of the Deliverables for Litigation Purposes, and (iv) any breach or violation of Sections 24-28 above. Further, the Client shall indemnify Supplier in full in respect of any loss, expense or damage incurred by Supplier as a result of (i) a violation of law by the Client, and (ii) any claim of intellectual property rights infringement by any third party, to the extent that such loss, expense or damage arises from information or data supplied to Supplier by the Client or by any other party on behalf of the Client.
36. Product Testing: In the event that for the purposes of the Services Supplier requires respondents to examine, test or use any products or services, the Client shall indemnify Supplier in full against any action or claim, in relation to liability, loss, damage, costs or expenses relating to such examination, test or use of such products or services.
37. In the event that Supplier or any of its employees, agents or subcontractors is served with or becomes subject to any subpoena, order or other legal process in a legal proceeding to which Supplier is not a party, seeking disclosure of any materials or information related to the Services or the Deliverables that Supplier renders or delivers to Client hereunder, then Client shall bear and/or reimburse Supplier for all costs and expenses, including but not limited to, reasonable legal fees and costs, related to Supplier's response, compliance with or resistance thereto.

LIABILITY

38. Supplier will use reasonable skill and care to ensure the accuracy of its reports, models and other presentations of the Services. As the nature of Services is based upon samples and statistical treatment of information, Supplier does not warrant the total accuracy of the Services or the data contained therein. Supplier does not predict or assure any particular substantive results of the Services in advance, nor does Supplier accept any liability for (i) Client's interpretation of Supplier's reports or of other data furnished to Client by Supplier, (ii) any errors caused by errors in data provided to Supplier, (iii) improper use of simulation software or improper interpretation of simulation software results by Client, or (iv) resale of survey results or other data by Client. Supplier will use commercially reasonable efforts to meet all project deadlines, but it does not guarantee meeting those deadlines. All time frames set forth in the Proposal with respect to the timing of the Services are approximations.
39. The Client acknowledges that it has entered into the Agreement in reliance only on the representations, warranties promises and terms contained in the Agreement and, save as expressly set out in the Agreement, Supplier shall have no liability in respect of any other representation, warranty or promise made prior to the date of the Agreement unless it was made fraudulently.
40. Except as expressly provided in these T&Cs and to the fullest extent permitted by law, Supplier hereby disclaims all warranties, conditions or other terms implied by statute or common law with respect to the Services and the Deliverables, including but not limited to any implied warranty of fitness for purpose.
41. Supplier excludes any liability of loss of contract, loss of profit, loss of revenue and loss of business, whether direct or indirect, and any incidental, indirect, exemplary, special or consequential loss or damage of any kind whatsoever arising out of or in connection with the contract whether or not such party was advised of the possibility of such damage and whether based in breach of contract, tort or any other theory at law or in equity.
42. Under no circumstances shall Supplier be responsible for failure to provide the services or for its delay in performance in accordance with this Agreement due to any event or condition, not existing as of the date of signature of this Agreement or not reasonably within the control of Ipsos as of such date, which prevents in whole or in material part the performance by Ipsos of its obligations

hereunder ("**Force Majeure**"). Without limiting the foregoing, the following shall constitute events or conditions of Force Majeure: acts of State or governmental action, terrorism, riots, disturbances, war, strikes, lockouts, slowdowns, prolonged shortage of energy supplies, epidemics/pandemics, fire, flood, hurricane, typhoon, earthquake, lightning and explosion or any other cause beyond Supplier's reasonable control. Should an event of Force Majeure last for more than thirty (30) days, then Supplier shall have the right to terminate the provision of work according to these T&Cs, this Agreement or the relevant Sales Order without liability to Client. Unless termination has occurred as set forth herein, both parties' obligations hereunder shall resume upon the cessation of the event of Force Majeure.

43. The maximum liability of Supplier for any breach of these T&Cs shall be limited to 125% of fees received by it in relation to the research which is the subject of the claim.

44. Nothing in these T&Cs shall limit or exclude either party's liability for: a) death or personal injury caused by its negligence; b) its fraud or wilful default; c) breach of Data Protection Legislation; and d) anything else which it cannot by law limit or exclude its liability.

TERMINATION

45. Either party shall have the right to terminate the Agreement with immediate effect, at any time, if the other party fails to perform any material obligation or to cure a material breach, subject to the breaching party receiving written notice of such failure to perform or material breach and provided further that such failure to perform or breach is not cured within fifteen (15) business days of receiving such notice. Clauses 17 - 52 shall survive the termination of this Agreement, save that if the Agreement is terminated by Supplier for default of the Client, the Client shall have no rights to use and Supplier shall retain all rights in the Deliverables.

GENERAL

46. Any notice to either party under these T&Cs shall be in writing signed by or on behalf of the party giving it and shall, unless delivered to a party personally, be left at or sent by prepaid first class post, prepaid recorded delivery or fax to the address of the party as notified in writing from time to time.

47. Nothing in this Agreement shall create a partnership or joint venture between the parties or render a party the agent of the other nor shall a party hold itself out as such (whether by an oral or written representation or by any other conduct).

48. No express or implied term of this Agreement is enforceable pursuant to the Contracts (Rights of Third Parties) Act of 1999 by any person who is not a party to it.

49. If either party fails to fully exercise any right, power or remedy under this Agreement, such right, power or remedy shall not be waived. No express waiver or assent by either party with respect to any breach or default under any provision of this Agreement shall constitute a waiver or assent with respect to any subsequent breach or default under that or any other provision. No waiver shall be effective unless in writing signed by the party waiving its rights hereunder.

50. To the extent that any provision of the Agreement is found by any court or competent authority to be invalid, unlawful or unenforceable in any jurisdiction, that provision shall be deemed not to be a part of these T&Cs, it shall not affect the enforceability of the remainder of these T&Cs nor shall it affect the validity, lawfulness or enforceability of that provision in any other jurisdiction. If a court or other decision-maker should determine that any provisions of this Agreement is overbroad or unreasonable, such provision shall be given effect to the maximum extent possible by narrowing or enforcing in part that aspect of the provision found overbroad or unreasonable.

51. This Agreement together with any documents annexed hereto or referred to herein sets out the entire agreement and understanding between the parties and supersedes all prior agreements, understandings or arrangements (whether oral or written) in respect of the subject matter of this Agreement and shall not be modified except in a writing signed by both parties.

52. These T&Cs shall be governed by and construed in accordance with English law and shall be subject to the exclusive jurisdiction of the courts of England.

APPENDIX 1 – Data Processing Obligations of the Client and Supplier

DEFINITIONS

Applicable Laws: means:
To the extent the UK GDPR applies, the law/s of the United Kingdom.; and/or
To the extent EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject.

Applicable Data Protection Laws: means:
To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data.
To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Supplier is subject, which relates to the protection of Personal Data.

Client Personal Data: any Client provided Personal Data which the Supplier processes in connection with the agreement to which this Appendix 1 is attached, as the Client's Processor.

EEA: the European Economic Area.

EU GDPR: the European Union's General Data Protection Regulation (*(EU) 2016/679*) as amended from time to time.
Purpose: the purposes for which the Client Personal Data are processed, as set out in clause 1.5(a)**.**

Supplier Group Affiliate: any entity that directly or indirectly controls, is controlled by, or is under common control with the Supplier.

Supplier Personal Data: any Personal Data which the Supplier processes **in** connection with this agreement as a Controller.

UK GDPR: has the meaning given to it in the Data Protection Act 2018 as amended from time to time.

1. DATA PROTECTION

1.1 For the purposes of this Appendix, the terms **Controller, Data Protection Impact Assessment, Processor, Joint Controller, Data Subject, Personal Data, Personal Data Breach, Supervisory Authority** and **Processing** shall have the meaning given to them in the UK GDPR.

1.2 Both parties will comply with all applicable requirements of Applicable Data Protection Laws. This Appendix is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Applicable Data Protection Laws.

1.3 Where Client Personal Data is transferred to the Supplier, without prejudice to the generality of clause 1.2, the Client will ensure that it and/or the organisation that supplies the Client Personal Data has the necessary appropriate legal basis and notice(s) in place to enable lawful transfer of Client Personal Data to the Supplier for the duration and purposes of this Appendix.

1.4 In relation to the Client Personal Data, Schedule 1 sets out the scope, nature and purpose of Processing by the Supplier, the duration of the Processing and the types of Personal Data and categories of Data Subject.

1.5 in relation to Client Personal Data and without prejudice to the generality of clause 1.2 the Supplier shall:

(a) process the Client Personal Data only on the documented instructions of the Client and only for the purposes set out in Schedule 1, unless the Supplier is required otherwise by Applicable Laws. Where the Supplier is relying on Applicable Laws as the basis for Processing Client Personal Data, the Supplier shall notify the Client of this before performing the Processing required by the Applicable Laws unless those Applicable Laws prohibit the Supplier from so notifying the Client on important grounds of public interest. The Supplier shall use reasonable endeavours to inform the Client if, in the opinion of the Supplier, the instructions of the Client infringe Applicable Data Protection Laws;

(b) implement the technical and organisational measures set out in Schedule 2 to protect against unauthorised or unlawful Processing of Client Personal Data and against accidental loss or destruction of, or damage to, Client Personal Data, which the Client has reviewed and confirms are appropriate to the harm that might result from the unauthorised or unlawful Processing or accidental loss, destruction or damage and the nature of the Data to be protected, having regard to the state of technological development and the cost of implementing any measures;

(c) ensure that any personnel engaged and authorised by the Supplier to process Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

(d) assist the Client insofar as this is possible (taking into account the nature of the Processing and the information available to the Supplier), and at the Client's cost and written request, in responding to any request from a Data Subject and in ensuring the Client's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, Data Protection Impact Assessments and consultations with Supervisory Authorities or regulators;

(e) notify the Client without undue delay on becoming aware of a Personal Data breach involving the Client Personal Data;

(f) at the written direction of the Client, delete or return Client Personal Data and copies thereof to the Client on termination of the agreement unless the Supplier is required by Applicable Law to continue to process that Client Personal Data. For the purposes of this clause 1.5(f) Client Personal Data shall be considered deleted where it is put beyond further use by the Supplier; and

(g) maintain records as required under UK GDPR or as set out specifically herein.

1.6 Any audit or inspection permitted following a request for audit accepted by the Supplier, which the Supplier may grant at its absolute and sole discretion and where the Supplier is deemed as the Processor, is not intended to include:

(i) any information related to the Supplier's provision of services to other clients or other client's Data; or

(ii) Supplier's general operating costs, overhead costs, or salary, timecards or other employee, personnel, and/or individual compensation records, or Supplier's profit and loss reports or other corporate records of Supplier.

1.7 The Client agrees that any agreed audit or access to Supplier's premises, in accordance with clause 1.6, will be in a manner that minimises interference with the Supplier's business operations, and that any request by the Client for an audit or access to the Supplier's premises may not be granted by the Supplier more than once in any 12-month period.

1.8 Where requested or required by the Supplier, the Client shall provide its authorisation for the Supplier or Supplier Group Affiliate/s to appoint Processors to process the Client Personal Data, provided that the Supplier or Supplier Group Affiliates:

(i) shall ensure that the terms on which it appoints such Processors comply with Applicable Data Protection Laws, and are consistent with the obligations imposed on the Supplier in this Appendix;

(ii) shall remain responsible for the acts and omission of any such Processor as if they were the acts and omissions of the Supplier; and

(iii) shall inform the Client of any intended changes concerning the addition or replacement of the Processors as listed in Schedule 2, thereby giving the Client the opportunity to object to such changes provided that if the Client objects to the changes and cannot demonstrate, to the Supplier's reasonable satisfaction, that the objection is due to an actual or likely breach of Applicable Data Protection Law, the Client shall indemnify the Supplier for any losses, damages, costs (including legal fees) and expenses suffered by the Supplier in accommodating the objection; and

(iv) transfer Client Personal Data outside of the UK and EEA as required for the Purpose, provided that the Supplier shall ensure that all such transfers are effected in accordance with Applicable Data Protection Laws. For these purposes, the Supplier shall promptly comply with any reasonable request of the Client, including any request to enter into standard contractual clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the Commissioner from time to time (where the UK GDPR applies to the transfer), if these are not already in place.

1.9 To the extent the parties act as Joint Controllers in respect of any Personal Data pursuant to the agreement, to which this Appendix is attached, the parties have agreed to allocate responsibility for each of their Controller obligations under Applicable Data Protection Laws in accordance with Schedule 3.

1.10 The Client hereby indemnifies, and shall keep indemnified, the Supplier from and against any and all costs, damages and expenses of any kind arising from any claim or demand brought by any person, Data Subject or Supervisory Authority as a result of any breach or alleged breach by the Client of any Applicable Data Protection Law or its obligations under this Appendix 1. This indemnity shall not be subject to any limits or exclusions of liability that may otherwise apply, or be imposed, under the agreement to which this Appendix is attached.

Schedule 1 **Particulars of the Processing**

Subject matter of the Processing of Personal Data	The Personal Data transferred concern the following categories of Data Subjects: (*)
Duration of the Processing of Personal Data	Supplier will process Personal Data during the term of the agreement to which this Appendix applies.
Nature of the Processing of Personal Data	(*)
Purpose of the Processing of Personal Data	Supplier will process Personal Data of data subjects for the purpose of providing the services in accordance with the agreement to which this Appendix applies, including: Market research Client satisfaction survey Employee survey (other*)
Categories of Personal Data being processed	Client customer data Client employee data (other *)
Location of Personal Data Processing	[If the location of any Processing of Personal Data is outside of any area considered to be adequate by the originating jurisdiction, such location must be specifically identified as such. E.g. the list of countries having an adequacy decision issued by the European Commission are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay). Other jurisdictions have their own adequacy decisions and/or requirements. If no transfer will be from the European Economic Area (EEA) to outside of the EEA or the countries listed above, the following sentence shall be included: "No Personal Data will be transferred outside the area providing an adequate
Data Protection Officer or when not applicable any other person acting as single point of contact on privacy or data protection matters	For Supplier: Catherine Bolton, dpo.unitedkingdom@ipsos.com For {Client}: {name and email address}
(*) or *	*Please specify or delete as appropriate*

Processors List **

Processor(s) Name	**Location**	**Type of Processing**
[To Be Updated]	[To Be Updated]	[To Be Updated]

[Add detail of any known Processors (including other Ipsos companies) who will process the Personal Data. Include a description of what each processor will do with the data (e.g. host, provide support, etc.)

***Any modification in the Processor listing shall be agreed in writing between the parties, either through an Amendment to this Agreement or included in the applicable Sales Order or other relevant project agreement. If only the category of Processor is known, but the specific processor has not yet been selected, state the category of Processor and likely location(s).*

Schedule 2 - Supplier ("Ipsos MORI") Technical and organisational measures

The Supplier and all sub-processors agreed with the Client and as listed in Appendix 3 will have in place appropriate organisational and technical measures to safeguard the Personal Data being processed under this data transfer agreement. The organisational, operational and technological processes and procedures adopted are required to comply with the requirements of ISO/IEC 27002 (ISO/IEC 17799) as appropriate to the services being provided. Ipsos MORI will use ISO/IEC 27002 as a basis for auditing compliance with the guarantees Ipsos MORI provides in relation to this obligation.

The measures in place will include the following minimum mandatory requirements:

Organizational Safeguards

- Ipsos MORI has an appointed data protection officer who has data protection and information security responsibilities set out as part of her duties and heads up a dedicated Compliance Department.
- Ipsos MORI will appoint a representative in the Union to meet EU GDPR requirements.
- Physical access to the building is limited by various access control mechanisms (e.g. key cards) and in most cases entrances to Ipsos MORI's offices are staffed by receptionists/security staff.
- Ipsos MORI's employees are instructed on data protection and information security matters upon commencing employment with Ipsos MORI and are subject to confidentiality obligations.
- Ipsos MORI's employees are not permitted to record Personal Data on a storage medium (e.g. disk) to enable them to re-access the information in premises that are not controlled by Ipsos MORI. In the event that Personal Data is held in hard copy format, any employees dealing with such Personal Data operate a clear desk policy, so that no Personal Data is left unattended in their absence. Personal Data in hard copy form is stored securely to prevent any unauthorized access.
- Ipsos MORI has business continuity plans in place, which are tested annually.

Information Security Risk Management

- Ipsos MORI periodically assesses risk within Information Technology specifically toward assets associated/involved in the services/products delivered. The implemented risk management framework is in agreement with the requirements of the ISO 27001 & ISO 27002.

Information Security Policy

- Ipsos MORI has in place an information security policy and other additional policies to ensure that controls are in place.
- Ipsos MORI regularly review its information security policy.
- Ipsos MORI follows Information Security programmes that are based on the following frameworks:
- ISO 27001 & ISO 27002 standards (Ipsos MORI is certified to ISO 27001)

Asset Management

- Ipsos MORI has documented and implemented rules with regards to acceptable use of assets.

Human Resources Security

- Ipsos MORI ensures that employees, contractors, and subcontractors who access Ipsos MORI assets are screened prior to employment; this meets the UK HMG Baseline Personnel Security Standard. Screening includes Criminal, financial (where applicable), employment background screening processes, where applicable with legislation.
- Ipsos MORI has processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential, or Personal information.
- Ipsos MORI ensures that an Information Security awareness campaign is provided to everyone who has access to Ipsos MORI assets.
- Ipsos MORI ensures that all user IDs, tokens or physical-access badges are assigned to a unique Ipsos MORI employee or Ipsos MORI subcontractor.
- Ensure all user/system/service/administrator accounts and passwords are never shared.

Physical and Environmental Security

Ipsos MORI assets are protected from:

- Natural disasters,
- Theft, physical intrusion, unlawful and unauthorized physical access,
- Ventilation, Heat or Cooling problems, power failures or outages.

Operations Management

Network Security:

Ipsos MORI deploys an intrusion detection system in the data centre monitoring the perimeter points, additional controls include layered anti-virus approach.

System Security:
Ipsos MORI has processes in place to apply and manage security updates, patches, fixes upgrades, (collectively referred to as "Patches") on all Ipsos MORI IT systems.

Ipsos MORI ensures that Malware, Virus, Trojan and Spyware protection programs are also deployed on IT systems.

Disaster recovery

- Ipsos MORI has appropriate disaster recovery measures to ensure that the Personal Data it processes can be re-instated in the event of loss or destruction of that data.
- The disaster recovery plan which will implement the disaster recovery measures defines RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives) where appropriate to the service being provided.
- Ipsos MORI reviews these technical safeguards periodically to ensure their continued suitability in light of the data it processes and technological advances.

Data management

Data Security

- Confidential information is encrypted and encryption must meet a minimum standard of AES-256-bit encryption.
- If a password/passphrase is used in the encryption of the document, the password/passphrase for the encrypted document is communicated, either:
  Face to face, or
  By phone or SMS, or
  A previously agreed password/passphrase

Transferring of Data
Acceptable Methods of Data Transfer:

- Secure File Transfer Protocol (sftp) – tcp port 22.
- HTTPS – tcp port 443.
- Suitable access controls in place

Handling of Data

- Ipsos MORI has in place documented information labelling and handling procedures, that must be followed by all employees.
- Only those staff assigned to a specific project for which the sample is intended may handle/ have access to that the Exporter's data.

Storage of Data

- Exporter's sample is stored on a server that is physically secured and is only accessed by authorized staff. Ipsos MORI stores Exporter's sample on a server that is protected behind a firewall and that is properly patched with the latest OS and Security patches.

Data destruction process

Ipsos MORI assures that:

- Working storage media will either be wiped, shredded, stored or degaussed;
- Non-working storage media will be stored securely and shredded.
- Industry best practice standards to be used.

Data Breach Procedure
In the event that any Personal Data supplied to Ipsos MORI by Exporter is accidentally or unlawfully destroyed, lost, altered, or an unauthorised disclosure or access to Personal Data occurs, Ipsos MORI will carry out the following incidence response as soon as they become aware:

- Ipsos MORI shall notify the Exporter of the breach.
- Ipsos MORI will immediately launch an investigation into the data breach in line with its documented Personal Data Breach Procedures.
- Ipsos MORI will co-operate with the Exporter in the investigation and will share all relevant system logs and evidence with the Exporter.
- The investigation will include root cause analysis and recommendations for improving Information Security in order to prevent future incidences; this will be included in the final Personal Data Breach report.

Access Management

- Ipsos MORI uses authentication and authorization technologies for service, user and administrator level accounts.
- Ipsos MORI ensures that IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks are always performed using non-administrator user accounts.
- Ipsos MORI has a password policy and other standards in place.

Vulnerability Testing

- Ipsos MORI ensures that infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices

Information Security Incident Management

- Ipsos MORI ensures access and activity audit and logging procedures, including access attempts and privileged access, exist.
- Ipsos MORI ensures that logging includes all facility, application, server, network device and IDS/IPS logs are centrally managed and maintained.
- Ipsos MORI ensures that security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to Ipsos MORI assets.

Schedule 3 - Joint Controller Allocation of Responsibilities

Activity	Responsibility for making policy and decisions	Responsibility for implementing policy and decisions
Legal basis for Processing of personal data and of special categories of personal data (if any) (Article[s] 6, 9 and 10)		
Purposes for which Personal Data may be collected (Article 5(1)(b))		
Data minimisation (Article 5(1)(c))		
Data accuracy (Article 5(1)(d))		
Data storage limitation (Article 5(1)(e))		
Integrity and confidentiality (Article 5(1)(f))		
Accountability (Article 5(2))		
Information notices (Articles 13 and 14)		
Data subject rights (Articles 15 to 22)		
Data protection by design and default (Article 25)		
Appointment of processor (Article 28)		
Records of Processing activities (Article 30)		
Co-operation with Supervisory Authority (Article 31)		
Security of Processing (Article 32)		
Notification of data breach (Articles 33 and 34)		
Impact assessments (Articles 35 and 36)		