KANTAR AND CLIENT DATA PROTECTION AGREEMENT

This Data Protection Agreement (**DPA**) will be effective as at the date the Parties have executed the Main Agreement described below (**Effective Date**).

BACKGROUND

(A) This DPA is written on the basis that Kantar and the Client (together the Parties) will on the Effective Date enter into an agreement for services provided by Kantar to the Client that involves the processing of Personal Data or that the Parties have already entered into one or more of these agreements.

(B) In this DPA the term **Main Agreement** refers to each agreement referred to in paragraph A individually and if the Main Agreement is a framework the reference to a Main Agreement includes call-off contracts or SOWs made under it. Accordingly this DPA forms part of a Main Agreement entered into contemporaneously with this DPA and/or is supplemental to and amends any and all existing Main Agreements and their related SOWs.

(C) The Parties agree that these terms will supplement any existing privacy and data protection terms contained in the Main Agreement, and that the terms of this DPA and its annexes shall prevail to the extent of any conflict or inconsistency with any other terms of the Main Agreement relating to the Processing of Client Personal Data.

The Parties agree as follows:

1. **DEFINITIONS**

Capitalised terms not otherwise defined herein shall have the meaning given to them in the Main Agreement. In this DPA, the following terms shall have the meanings set out below unless the context otherwise requires:

1.1 **Affiliate** means, (a) in respect of Kantar, any entity (excluding Europanel) which, from time to time both: (i) directly or indirectly through one or more intermediaries, Controls, or is Controlled by, or is under common Control of, Kantar; and (ii) is trading as **Kantar** (and **Kantar Affiliate** shall be construed accordingly); and, (b) in respect of Client, any entity which is Controlled by **Client** (and **Client Affiliate** shall be construed accordingly).

1.2 **Client Personal Data** means any Personal Data Processed on behalf of the Client (as Controller) by Kantar (as a Processor) or by a Sub-processor pursuant to the Main Agreement.

1.3 **Control** means, in respect of any entity: (i) possession, direct or indirect through one or more intermediaries, of the power to direct the management or policies of such entity, whether through ownership of voting securities, by contract relating to voting rights, or otherwise; or (ii) ownership, direct or indirect through one or more intermediaries, of more than 50% percent of the outstanding voting securities or other ownership interest of such entity (and Controls and Controlled shall be construed accordingly).

1.4 **Controller** means the Party that alone or jointly with others determines the purposes and means of the Processing of Personal Data, unless the term "controller" (or cognate term under Data Protection Laws, such as (for example) "business" or "personal information processor") is defined under Data Protection Laws in which case the term "controller" shall have the same meaning as in Data Protection Laws, and its cognate terms shall be construed accordingly.

1.5 **Data Processing Particulars** means the description of Processing of Client Personal Data, in the same or similar form as set at the Annex to this DPA, as detailed within the Main Agreement (or relevant SOW) carried out in connection with the provision of Services under that Main Agreement (or relevant SOW).

1.6 **Data Protection Laws** means all applicable laws, rules and regulations in any relevant jurisdiction relating to the Processing of Personal Data and privacy including but not limited to the EU GDPR, the UK GDPR, US state privacy laws, and the PIPL.

1.7 **Data Subject** means an identified or identifiable natural personal to whom Personal Data relates, unless the term "data subject" (or cognate term under Data Protection Laws, such as (for example) "consumer" or "personal information subject") is defined under Data Protection Laws in which case the term "data subject" shall have the same meaning as in Data Protection Laws, and its cognate terms shall be construed accordingly.

1.8 **DPIA** means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, or similar risk assessment, pursuant to (and as set out in) Data Protection Laws.

1.9 **EU GDPR** means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.10 **EU SCCs** means the standard contractual clauses approved by European Commission decision 2021/915 on standard contractual clauses for the transfer of Personal Data to processors (pursuant to the EU GDPR) as amended or replaced from time to time.

1.11 **Independent Auditor** means an auditor from PwC, Deloitte, KPMG or EY (Ernst & Young) or another mutually agreeable internationally recognised auditing firm that is not employed on a contingency basis skilled and experienced in conducting audits related to data protection governance risk and compliance.

1.12 **Personal Data** means any information relating to an identified or identifiable natural person, unless the term "Personal Data" (or cognate term under Data Protection Laws, such as (for example) "personal information" or "personal identifiable information") is defined under Data Protection Laws in which case the term "Personal Data" shall have the same meaning as in Data Protection Laws, and its cognate terms shall be construed accordingly.

1.13 **Personnel** means either Party's stakeholders, directors, employees, agents, consultants, subcontractors, Contracted Processors, Sub-processors or other persons authorised by (i) either Party; (ii) their Affiliates; and / or (iii) their subcontractors engaged in the provision of Services.

1.14 **PIPL** means the Personal Information Protection Law of the People's Republic of China as adopted 20 August 2021.

1.15 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16 **Processor** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller, unless the term "Processor" (or cognate term under Data Protection Laws, such as (for example) "service provider" or "entrusted party") is defined under Data Protection Laws in which case the term "Processor" shall have the same meaning as in Data Protection Laws, and its cognate terms shall be construed accordingly.

1.17 **Restricted International Transfer** means a transfer of Client Personal Data that would be prohibited by the applicable Data Protection Laws in absence of the protection for the transferred Client Personal Data provided by a Restricted International Transfer Agreement.

1.18 **Restricted International Transfer Agreement** means the relevant standard contractual clauses (including but not limited to the EU SCCs or UK IDTA) or any other standard or non-standard contractual clauses required under Data Protection Laws (as established, amended or replaced from time to time).

1.19 **Sub-processor** means any person or entity appointed by Kantar as set out in clause 5 (Sub-processors) to Process Client Personal Data on behalf of Client in connection with the Main Agreement.

1.20 **Supervisory Authority** means a public authority or regulator established in a relevant jurisdiction for matters relating to the Processing of Personal Data and/or privacy.

1.21 **SOW** means a statement of work entered into by the Parties (or any of their respective Affiliates) to document their agreement in respect of any services, which is more specifically defined in the Main Agreement.

1.22 **UK GDPR** has the meaning given by section 3(10) and section 205(4) the UK's Data Protection Act 2018.

1.23 **UK IDTA** means the standard contractual clauses issued by the Information Commissioner's Office in the United Kingdom pursuant to UK GDPR (as amended or replaced from time to time).

1.24 For the purposes of this DPA where the context requires:

1.24.1 any reference to Parties shall be to the relevant parties to the relevant SOW (and Party shall mean any one of them)

1.24.2 any references to Client shall mean the relevant Client Affiliate that is a party to that SOW; and

1.24.3 any references to Kantar shall mean Kantar and, in respect of any SOW, the relevant Kantar Affiliate that is a party to that SOW.

2. PROCESSING OF PERSONAL DATA

2.1 Where the Main Agreement acts as a framework the Parties envisage that Kantar will provide a variety of different Services and that the Parties may collaborate and interact in a variety of ways. The Parties may agree specific provisions relating to the use of Personal Data in the delivery of specific Services and set them out in a SOW. If no specific provisions apply then the remaining provisions of this clause 2 shall apply by default

Parties acting as Independent Controller

2.2 If Kantar does not Process Client Personal Data but provides the relevant Services using its own data or data obtained from third parties then if any of that data is Personal Data Kantar may act as an independent Controller.

2.3 Where a Party acts as an independent Controller it shall:

2.3.1 comply with applicable Data Protection Laws in relation to such Personal Data; and

2.3.2 treat Personal Data obtained from the other Party or relating to employees or members of staff as Confidential Information under the Main Agreement.

Kantar acting as Processor

2.4 Except as set out in clauses 2.2 to 2.3, the Parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Controller, Kantar is the Processor, and that Kantar or Kantar Affiliates will engage Sub-processors pursuant to the requirements in clause 5 (Sub-processors). Kantar shall Process Client Personal Data on behalf of the Client in compliance with the Client's lawful instructions for the purposes described in the Data Processing Particulars (**Permitted Purposes**). Kantar shall not sell, share for purposes of cross-context behavioural advertising, license, or otherwise exchange Client Personal Data for monetary or other consideration.

2.5 If other Processing is required by local applicable law (including local laws in a relevant Sub-processor country), Kantar shall, to the extent permitted by law, inform Client of that legal requirement before such Processing.

2.6 The Client warrants that:

2.6.1 it has complied and will continue to comply with Data Protection Laws;

2.6.2 its instructions for the Processing of Personal Data shall at all times comply with Data Protection Laws;

2.6.3 all Client Personal Data has been and will continue to be collected and processed in accordance with the notice, consent and other requirements of Data Protection Laws (and where applicable, the collection and processing has been notified to the relevant authorities);

2.6.4 it has and will continue to have the right to transfer or provide access to the Client Personal Data to Kantar and the Sub-processors for the Permitted Purposes and that such Processing by Kantar and the Sub-processors will not breach Data Protection Laws; and

2.6.5 its instructions to Kantar in respect of the Processing of Client Personal Data are lawful and will not create legal or regulatory liability on the part of Kantar or any Sub-processor if followed.

3. SECURITY

3.1 Kantar shall maintain appropriate technical and organisational measures designed to protect the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to, Client Personal Data), confidentiality and integrity of Client Personal Data. Kantar shall regularly monitor compliance with these measures.

3.2 In addition, Kantar shall:

3.2.1 only involve Kantar Personnel to process Client Personal Data under the Main Agreement who have had appropriate training pertinent to the care and handling of Personal Data;

3.2.2 only authorise Kantar Personnel to process Client Personal Data if such person is subject to a duty of confidentiality (whether a contractual duty or a statutory duty or otherwise); and

3.2.3 ensure the reliability of Kantar Personnel to whom Kantar has provided access to Client Personal Data.

4. **RIGHTS OF DATA SUBJECTS**

4.1 Kantar shall to the extent legally permitted, notify Client if Kantar receives a request from a Data Subject, third parties, relevant data protection authorities in the relevant local jurisdiction or any other law enforcement authority, to exercise the Data Subject's privacy rights under applicable Data Protection Laws, including but not limited to the right of access, right to rectification, restriction of Processing, erasure (right to be forgotten), data portability, right to object to the Processing, or its right not to be subject to automated individual decision making (**Data Subject Request**).

4.2 Taking into account the nature of the Processing, Kantar shall in accordance with Client's reasonable instructions, assist Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws.

4.3 Client shall be responsible for any costs arising from Kantar's provision of such assistance or Kantar's compliance with this clause 4.

5. **SUB-PROCESSORS**

5.1 Client authorises Kantar and each Kantar Affiliate to use and continue to use Kantar Affiliates and existing Kantar Sub-processors as of the effective date of this DPA as Sub-processors, subject to Kantar and each Kantar Affiliate (in each case) meeting the obligations set out in this clause as soon as practicable.

5.2 Kantar shall and shall require Kantar Sub-processors to give Client prior written notice and details of the appointment of any new Kantar Sub-processor or any changes to existing Kantar Sub-processors, including details of the Processing to be undertaken by the new Kantar Sub-processor.

5.3 If, within ten (10) business days of receipt of that notice, Client notifies Kantar in writing of any objections (on reasonable grounds that relate to these DPA terms) to the proposed appointment, Kantar shall take reasonable steps to address the objections raised by the Client and provide Client with a written explanation of the steps taken. During such time Kantar or Kantar Sub-processor shall not appoint such new Kantar Sub-processor until such objections have been addressed.

5.4 If the Parties are unable to resolve Client's objections, Kantar shall not make such change and Kantar shall be entitled to suspend Processing in respect of the relevant Services and/or Kantar may treat the relevant Services as terminated by the Client for its convenience in which case the Client shall be responsible for reimbursing Kantar for any unavoidable committed costs incurred as a result of the termination.

5.5 New Kantar Sub-processors and / or any changes concerning Kantar Sub-processors will be set out in the Data Processing Particulars.

5.6 Kantar shall remain fully liable to the Client for the performance of Sub-processor obligations under this DPA**.**

6. **AUDIT**

6.1 Subject to the following terms, Kantar permits Independent Auditors appointed by Client to audit Kantar only to the extent the Main Agreement does not already provide the Client with audit or similar rights, and only to the extent required by the applicable Data Protection Laws. Such information derived from the audit is referred to in this clause 6 as **Audit Information**.

6.2 Independent Auditors shall upon giving Kantar reasonable written notice (minimum thirty (30) calendar days) have supervised and controlled access to relevant facilities at Kantar's service locations during business hours and they shall use reasonable endeavours to minimise disruption while exercising the rights of audit set out in this clause 6. Client shall notify Kantar of the identity of any visiting Independent Auditors to ensure they have entered into appropriate confidentiality agreements beforehand, in a form approved by Kantar (such approval not to be unreasonably withheld or delayed).

6.3 Audits shall take place no more than once in any calendar year unless and to the extent that Client (acting reasonably and in good faith) has reasonable grounds to suspect any material breach of this DPA by Kantar, in which case Client and Kantar will agree timescales for the audit. Costs of the audit, including appointment of the Independent Auditor, will be borne by Client.

6.4 Kantar shall reasonably cooperate with Client in relation to any audit request by Client. Unless otherwise set out in this clause 6, audits shall be subject to the confidentiality obligations set forth in the Main Agreement.

6.5 Kantar shall be entitled to a reasonable time to review and retain a copy of any audit report, prepared by Independent Auditor and to consult the Independent Auditor on the content, prior to the audit report being submitted to Client. For avoidance of doubt, all Audit Information obtained by Client or an Independent Auditor pursuant to any audit shall be maintained in confidence by Client and its Independent Auditor and may not be disclosed to any third party, including, without limitation, any other agents or representatives of Client except to the extent necessary to assert or enforce any of the Client's rights under this DPA or where it is required to be disclosed by Data Protection Laws, by any Supervisory Authority or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives Kantar as much notice of this disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause, it takes into account the reasonable requests of Kantar in relation to the content of this disclosure.

6.6 Neither the Independent Auditor nor Client shall be permitted to perform penetration tests, vulnerability scans, or otherwise interrogate Kantar's network or information technology systems.

6.7 In no circumstances shall Client or the Independent Auditor have access to:

6.7.1 individual payroll and Kantar Personnel files;

6.7.2 individual expenditure or records relating to Kantar's business or its other clients;

6.7.3 Kantar's confidential information or trade secrets;

6.7.4 any of Kantar's overhead costs; or

6.7.5 Kantar's server rooms or IT systems.

7. **DATA INCIDENT MANAGEMENT AND NOTIFICATION**

7.1 Kantar shall notify Client's relevant business contact without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Client Personal Data, transmitted, stored or otherwise Processed by Kantar or its Sub-processors which results in any actual loss or misuse of Client Personal Data (a **Data Incident**).

7.2 Kantar shall make reasonable efforts to identify the cause of such Data Incident and take those steps as Kantar deems necessary and reasonable in order to remediate the cause of such a Data Incident to the extent the remediation is within Kantar's reasonable control.

7.3 Kantar shall have no liability for costs incurred arising from a Data Incident except where Kantar has deliberately or negligently failed to comply with the technical and organisational measures referred to in Annex 1. Each Party shall use all reasonable endeavours to mitigate costs incurred as a result of a Data Incident caused by the other Party.

7.4 If the Client has caused the Data Incident, the Client shall be responsible for costs, including Kantar's costs, reasonably incurred to rectify the Data Incident, including in circumstances in which such Data Incident arises as a result of the Client's instructions to Kantar, or if the Client requires Kantar to notify Data Subjects and / or Supervisory Authorities as set out in clause 7.5.

7.5 In the event of a Data Incident, Client shall be responsible for notifying Data Subjects and or Supervisory Authorities, unless the Client has instructed Kantar to do so or Kantar is otherwise required to do so under Data Protection Laws. Before any such notification is made, Client shall consult with and provide Kantar an opportunity to comment on any notification made in connection with a Data Incident.

8. **RETURN AND DELETION OF CLIENT PERSONAL DATA**

8.1 Kantar shall, at any time at the Client's request delete (so far as is reasonably practicable and other than any back-up copies) or return all Client Personal Data, except that this requirement shall not apply to the extent that:

8.1.1 Kantar or Kantar Affiliates are required to retain Client Personal Data for compliance with applicable laws or regulatory requirements.

8.1.2 Client Personal Data is required by Kantar to comply with any continuing obligations under the Main Agreement.

8.1.3 Client Personal Data is archived on back-up systems, provided that such copies are kept confidential and secure in accordance with the relevant Main Agreement terms.

9. **DATA PROTECTION IMPACT ASSESSMENT**

Upon Client's request, Kantar shall provide Client with reasonable cooperation and assistance, at Client's cost, needed to fulfil Client's obligation under Data Protection Laws to carry out a DPIA (to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to Kantar), to allow the Client to comply with its obligations under Data Protection Laws as a Controller in relation to data security and related consultations.

10. **RESTRICTED INTERNATIONAL TRANSFERS AND PROCESSING IN THIRD COUNTRIES**

10.1 Kantar shall ensure that the applicable Restricted International Transfer Agreement terms shall apply on commencement and to the extent of any Restricted International Transfer.

10.2 The Parties acknowledge that their compliance with the preceding sub-clause does not obviate the need to take other steps to justify Restricted International Transfers where necessary under applicable Data Protection Laws, which may include as appropriate: (i) carrying out a transfer risk assessment / transfer impact assessment as the case may be; (ii) entering into additional supplementary security measures arising from the transfer risk assessment / transfer impact assessment (iii) notifying or obtaining the consent of the Data Subjects whose Personal Data is transferred; or (iv) where required, notifying, or obtaining the prior approval of, applicable Supervisory Authorities; or (v) where required, notifying or obtaining the prior approval of works councils or similar employee representatives and the Parties shall resolve to comply with such other steps and procure that they are documented as appropriate. Nothing in this DPA shall be construed to prevail over any conflicting clause of any Restricted International Transfer Agreement.

11. **LIMITATION OF LIABILITY**

Each Party and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to a breach of its obligations under this DPA, whether in contract, tort or under any other theory of liability is subject to the liability terms in the Main Agreement, and any reference in such terms to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Main Agreement.

12. **GOVERNING LAW**

The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Main Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity, and this DPA and is governed by the laws of the country or territory stipulated for this purpose in the Main Agreement.

ANNEX

FORM OF DATA PROCESSING PARTICULARS

In accordance with the data protection terms for the Main Agreement, the parties agree that in accordance with Article 28(3) of the GDPR, the particulars of the Processing of Personal Data for the performance of the Services are as follows:

	Details
Subject matter	
Duration of processing	
Purposes and nature of processing	
Categories of personal data	
Categories of sensitive personal data	
Categories of data subject(s)	