KANTAR AND CLIENT DATA PROTECTION AGREEMENT

This Data Protection Agreement (**DPA**) will be effective as at the date the Parties have executed the latest in time of any 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.

(A) In this DPA the term **Main Agreement** refers to the agreement or to each agreement described in paragraph A individually (if more than one) 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 supplementary contracts or SOWs.

(B) The Parties agree that these terms will supplement any existing privacy and data protection terms contained in any 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 a 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 incorporated entity which, from time to time directly or indirectly through one or more intermediaries, Controls, or is Controlled by, or is under common Control of 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 equivalent 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 II 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 federal and 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 equivalent 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 equivalent 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 on 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 7 (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 (or similar engagement document) 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 DPA shall apply by default

3. PARTIES ACTING AS INDEPENDENT CONTROLLER

3.1 If Kantar provides the relevant Services using its own survey respondents, data, or data or survey respondents obtained from third parties, then if any of that data is Personal Data Kantar shall act as an independent Controller. To the extent that the Client receives (or is given access to) any Personal Data from Kantar, the Client shall also act as an independent Controller. A further description of the envisaged circumstances where the Parties shall act as independent Controllers is detailed at Annex IV. In such circumstances, clauses 4 to 11 (inclusive) of this DPA shall not apply.

3.2 In the circumstances described at clause 3.1, unless otherwise agreed, the Parties acknowledge it is not the intention of Kantar to supply any Personal Data to the Client. Therefore, in such circumstances, the Client shall not itself or by using a third party take any action or undertake any processing that could enable it directly or indirectly to discover the identity of survey respondents from data provided to the Client, including (but not limited to) matching the survey responses with other data controlled by or in the possession of the Client or any third party.

3.3 In the circumstances described at clause 3.1, it is agreed that (and in the case of the Client, to the extent that it receives (or is given access to) Personal Data from Kantar):

3.3.1 the Parties shall comply with applicable Data Protection Laws in relation to such Personal Data;

3.3.2 the Parties shall treat Personal Data obtained from the other Party or relating to employees or members of staff as Confidential Information under the Main Agreement;

3.3.3 the Parties 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, the Personal Data), confidentiality and integrity of the Personal Data, and shall regularly monitor compliance with these measures;

3.3.4 the Client shall not share Personal Data, collect follow-up data from survey respondents or Process the Personal Data of the survey respondents except for the purposes referred to in the SOW ("**Further Processing**") unless it is expressly permitted to do so in the relevant SOW. For clarity, this prohibits Processing for the purposes of advertising, sales and marketing, or otherwise attempting to influence the opinion of the survey respondents as consumers. The scope of permitted Processing and the Personal Data that is being Processed shall be defined separately for each type of project in the relevant SOW;

3.3.5 when providing the Services, Kantar may partner with other operators of market research panels (a "Panel") and the Client acknowledges that the creation and maintenance of a Panel is a business asset requiring significant investment. Accordingly, the Client shall not Process the Personal Data of a survey respondent, or member of a Panel, or have any contact with, or cause or permit any other person to have contact with, a survey respondent or member of a Panel in an attempt to encourage the panellist to leave any Panel, of which they are a member at the time of the contact, or to join another Panel or to perform an activity not specifically within the scope of the permitted Processing referred to in a SOW in which they are participating;

3.3.6 the Client shall only process Personal Data on the basis of voluntary, informed and expressly given consent of the Data Subjects

3.3.7 the Client shall ensure that all Personal Data is deleted promptly, and in any event within 60 days, following the end of the relevant Services; and

3.3.8 the Parties shall notify the other party without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data (a "Data Incident") and, upon request, provide the other party with all reasonably requested details of, and assistance with, the Data Incident, including for the purposes of any requirement to notify a relevant data protection authority or the Data Subjects.

4. KANTAR ACTING AS PROCESSOR

4.1 If Kantar provides the relevant Services using survey respondents obtained or sourced by the Client, then, with regard to the Processing of Personal Data (being Client Personal Data), the Client is the Controller and Kantar is a Processor on behalf of the Client. A further description of the envisaged circumstances where Kantar shall act as a Processor is detailed at Annex IV. In such circumstances, the following clauses of this DPA shall apply. Where the Client is acting as a Processor on behalf of a third-party Controller, the same terms apply as if Kantar is a sub-Processor ultimately on behalf of the third-party Controller.

4.2 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.

4.3 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.

4.4 The Client warrants that:

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

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

4.4.3 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);

4.4.4 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

4.4.5 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.

5. SECURITY

5.1 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.

5.2 In addition, Kantar shall:

5.2.1 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;

5.2.2 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

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

6. RIGHTS OF DATA SUBJECTS

6.1 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**).

6.2 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.

6.3 Client shall be responsible for any costs arising from Kantar's provision of such assistance or Kantar's compliance with this clause 6.

7. SUB-PROCESSORS

7.1 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.

7.2 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.

7.3 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.

7.4 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.

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

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

8. **AUDIT**

8.1 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 8 as **Audit Information**.

8.2 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 8. 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).

8.3 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.

8.4 Kantar shall reasonably cooperate with Client in relation to any audit request by Client. Unless otherwise set out in this clause 8, audits shall be subject to the confidentiality obligations set forth in the Main Agreement.

8.5 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.

8.6 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.

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

8.7.1 individual payroll and Kantar Personnel files;

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

8.7.3 Kantar's confidential information or trade secrets;

8.7.4 any of Kantar's overhead costs; or

8.7.5 Kantar's server rooms or IT systems.

9. **DATA INCIDENT MANAGEMENT AND NOTIFICATION**

9.1 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**).

9.2 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.

9.3 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 III. Each Party shall use all reasonable endeavours to mitigate costs incurred as a result of a Data Incident caused by the other Party.

9.4 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 9.5.

9.5 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.

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

10.1 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:

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

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

10.1.3 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.

11. **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.

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

12.1 Kantar shall ensure that the applicable Restricted International Transfer Agreement terms shall apply on commencement and to the extent of any Restricted International Transfer, such as to any Sub-processors or Kantar Affiliates.

12.2 The Parties agree that the relevant Restricted International Transfer Agreement terms are incorporated by reference into this DPA and shall apply on commencement, and to the extent, of any Restricted International Transfer.

12.3 If the Parties are required to enter into Restricted International Transfer Agreement with each other:

12.3.1 the information needed to complete the clauses and annexes of the EU SCCs are set out in paragraph 1 (Options (for EU SCCs) and equivalent terms) in Annex 1;

12.3.2 Restricted International Transfers subject to Data Protection Laws of Switzerland will be subject to the EU SCCs with the following modifications: the competent supervisory authority in Annex 1.C under Clause 13 will be the Federal Data Protection and Information Commissioner; references to a "Member State" and "EU Member State" will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to "GDPR" in the SCCs will be understood as references to Data Protection Laws of Switzerland;

12.3.3 the information needed to complete the tables of the UK IDTA, or tables or options (or similar unpopulated information) of any other Restricted International Transfer Agreement not already covered by above subclauses, is set out in the Main Agreement, including the Data Processing Particulars of this DPA. Where unpopulated, references to an applicable Supervisory Authority shall mean the relevant Supervisory Authority of the country of the applicable Data Protection Law, and references to an applicable governing law and/or choice of forum shall mean the law and courts of the country of the applicable Data Protection Law;

12.3.4 notwithstanding the fact that the Restricted International Transfer Agreement(s) are incorporated by reference without the signature pages actually being signed by the data importer and data exporter, the Parties agree that its respective execution of the Main Agreement is deemed to constitute its execution of the Restricted International Transfer Agreement on behalf of the data exporter/data importer (as applicable). However, where incorporation by reference is not permitted by law, the Parties agree to co-operate to promptly enter into any relevant Restricted International Transfer Agreement(s), separately to this DPA.

12.3.5 the Parties shall cooperate with each other to carry out the Supplementary Security Measures set out in paragraph 3 (Supplementary Security Measures) of Annex 1.

12.4 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.

13. **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.

14. **GOVERNING LAW**

The Parties to this DPA agree 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 I

RESTRICTED INTERNATIONAL TRANSFER AGREEMENTS

1. Modules for SCCs

1.1 In respect to the EU SCCs (including those subject to the Data Protection Laws of Switzerland) entered into by the Parties:

1.1.1 Module One (Controller to Controller) will apply to a Restricted International Transfer both Parties act as Controllers.

1.1.2 Module Two (Controller to Processor) and Module Four (Processor to Controller) will apply to a Restricted International Transfer where the Client is a Controller and Kantar is a Processor, as applicable to the direction of the transfer.

1.1.3 Module Three (Processor to Processor) will apply to a Restricted International Transfer where both Parties act as Processors.

2. Options for EU SCCs and equivalent terms

The Parties make the following options which shall apply to each Restricted International Transfer under the EU SCCs (including those subject to the Data Protection Laws of Switzerland) entered into by the Parties.

2.1 **Clause 7 (Docking clause)** shall apply with regards to each Data Importer.

2.2 **Clause 9 (Use of Sub-processors).** Option 1 shall apply. The time period shall be 60 days.

2.3 **Clause 13(a) (Supervision)** means the Supervisory Authority in Ireland (the Data Protection Commission).

2.4 **Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction)**. Option 2 shall apply. The governing law and courts in Ireland shall apply.

2.5 **Annex I** shall be pre-populated with the relevant sections of Data Processing Particulars and the relevant details of the Parties in the Main Agreement (or relevant SOW). The role of data exporter and the data importer may vary between Kantar and the Client, subject to the direction of the transfer.

2.6 **Annex II** shall be pre-populated with the relevant TOMs and the Supplementary Security Measures detailed below in this Annex I.

2.7 **Annex III** shall to be pre-populated with the details of the relevant sections of Data Processing Particulars.

3. Supplementary Security Measures

2.1 The Parties shall cooperate with each other to carry out these Supplementary Security Measures in response to a public / private / regulatory authority order to access Client Personal Data or surveillance order (**Order**).

2.2 The recipient Party shall notify the other Party without undue delay of any Order.

2.3 To the extent permitted by law, where acting as a Processor, Kantar will not attempt to respond in detail to such a request without the relevant Controller's prior written consent. Kantar may, however, provide generic information to public / private / regulatory authority as part of its obligations to cooperate without consulting or obtaining the prior consent of the relevant Controller.

ANNEX II

FORM OF DATA PROCESSING PARTICULARS

In accordance with the data protection terms for the Main Agreement, the parties agree that the particulars of the Processing of Personal Data for the performance of the Services are as follows. However, the particulars of processing may be supplemented or replaced by particulars agreed in a SOW. In case of any conflicting information, the particulars in the SOW will apply.

	Details
Controller	The Client and/or Kantar, according to Annex IV and any relevant SOW.
Processor	Kantar, where applicable according to Annex IV and any relevant SOW.
Subject matter	The provision of the Services to the Client.
Duration of processing	The term of the Main Agreement.
Purposes and nature of processing	Market research services and recruitment of survey respondents.
Categories of personal data	Full name, contact information, age, gender, employment information, demographic information, video recordings, and any information collected in the market research survey (such as consumer opinions), as instructed by the Client.
Categories of sensitive personal data	Demographic information (such as race/ethnicity), health and medical information, and any information collected in the market research survey, as instructed by the Client.
Categories of data subject(s)	Survey respondents provided by the Client, which may include the Client's customers.
Approved Sub-Processors	As detailed as subcontracting parties in the relevant SOW.

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES

This Annex III provides an overview of the approach we take to deliver a security programme in-line with industry best practice. This document is applicable to both on-premises and cloud environments. All guidelines, policies, and procedures outlined herein are relevant and enforceable across both deployment models.

1. **Controls Management**

Kantar has defined a Technology and Cyber Controls Framework to ensure control over the definition, creation, and implementation of controls and risk management. This Framework informs how managing cyber and technology risk is approached, implemented, monitored, and governed globally at Kantar and defines the statement of applicability (the scope). Kantar takes various factors into consideration as part of our prioritisation and oversight including threats and client expectations.

2. **Policies and Standards**

Kantar's Information Security Policy Framework consists of a global policy, maintained within the Kantar Policy Book, which applies to all employees. The global 'Cyber Security for Users' policy is supported by multiple security Standards. The Policy Framework defines the requirements for developing, reviewing, updating, and publishing policies, standards, and guidelines. Reviews are conducted on an annual basis and may also be triggered by material changes in services, regulatory or compliance obligations.

Additionally, the Kantar Policy Book covers areas such as Business Principles, Protecting Personal Information, Anti-Bribery & Corruption, Data Ethics & Integrity, Anti Money Laundering, and Business Continuity.

3. **Asset Management**

Kantar maintains and updates asset information for IT hardware, software, and applications/systems, either on-prem or Cloud environments, following industry best practice, including tools for auto-discovery for assets. Hardware asset management includes, but is not limited to, device configuration management and build management documentation. Software Asset Management includes software inventories, source code repositories, and software configuration. Regular audits are implemented to ensure asset information is up-to-date and accurate, helping to identify any discrepancies or outdated information. Detailed lifecycle management processes are included for assets, from acquisition to disposal, ensuring effective management throughout their lifespan. Asset management processes are integrated with security protocols, including regular vulnerability assessments and patch management for all assets. Training is provided for staff on the importance of asset management and how to use the tools effectively, improving compliance and reducing risks.

4. **Training and Awareness**

Kantar has a mandatory culture and awareness programme for all staff. All mandatory training is monitored centrally by the Global Compliance function. The courses include, but are not limited to:

- Protecting Our Data – Security and Data Protection (mandatory for all)
- Preventing Bribery, Corruption and the Facilitation of Tax Evasion at Kantar (mandatory for all)
- Ethics at Kantar (mandatory for all)
- Role based training (i.e., Developers, Finance) (as needed)

5. Identity and Access Management (IAM)

Kantar's IAM Standard is in place to establish and maintain controls for appropriate identification, authentication, authorisation, and access governance/account management.

Access to Kantar resources and services are granted via a unique user identifier per account type with a complex password. Each user account is unique to an individual. Passwords conform to the following criteria:

- Remote sessions must be terminated after 15 minutes of inactivity
- No re-use of any of the previous 5 passwords on a user account
- Passwords on all accounts must be changed once a year
- All person accounts must have:
  - Passwords changed once a year
  - Multi-factor authentication at the point of access
  - Single sign-on support
- Default passwords must be changed
- Minimum interval of 24 hours between successful user account password changes
- Account is rendered non-functional after 5 consecutive failed authentication attempts
- Passwords must comply with the following minimum requirements:
  - 14 characters in length for standard, privileged and service accounts
  - Meet, at least, 3 of the following complexity requirements:
    - Uppercase character
    - Lowercase character
    - Numeric characters (0-9)
    - Special character

Access is subject to an appropriate level of approval, follows the principles of least privilege and is revoked promptly for individuals leaving the organisation. Accounts that have been dormant for ≥45 calendar days must be disabled.

In accordance with Kantar's IAM standard, privileged accounts are unique and separately managed.

6. Secure System Development Lifecycle (Secure SDLC)

Kantar's Secure SDLC Standard is in place to protect Kantar information assets and information systems by ensuring applications and associated systems are designed and developed to allow for the identification and mitigation of security-related issues.

Secure Development Environment

Environments must be segregated and secure for its development resources to work from. Access is restricted to authorised personnel and only contains test data or documentation associated with development activities.

Operations and Application Maintenance

Once released into the live environment, assigned development resources continually monitor and apply updates as required in-line with Kantar's security standards. Test and validation environments or duplicated data sources used during development are securely removed.

Change Management

Formal change management processes must be followed whenever a system or application is modified to avoid direct or indirect negative impacts that the change may impose.

Architectural/Security documentation

High and Low-level architectural documentation is required for all systems and applications developed.

Use of third-party development resources

Where it is necessary for Kantar to procure the services of an external organisation, the secure development practices of the third-party shall be fully assessed prior to procurement taking place.

Secure Decommissioning

During development activities, consideration shall be given to how the asset is to be retired and any live data associated with the application at that time is to be properly and securely managed.

7. Network Security

Kantar's Network Security Standard outlines the controls for network security requirements, ensuring communication networks and associated components supporting business processes are safeguarded and secure. Kantar's technical network controls include, but are not limited to:

- Next Generation Firewalls (NGFW), DDoS Solution, Proxies and Virtual Private Network (VPN), Web Application Firewall (WAF), where appropriate
- Endpoint Detection and Response (EDR) solutions are deployed on all endpoints
- Log integration with Security Incident and Event Management (SIEM) systems
- Packet inspection for inbound and outbound network traffic

Wireless network access is only permitted from approved Kantar corporate endpoints. Guest wireless access does not permit access to the organisation's corporate network.

8. Endpoint Device Security

Kantar's Endpoint Device Management Standard provides secure and controlled usage of endpoint devices for access to Kantar networks, to reduce risks of unauthorised access and compromise to sensitive data. Endpoint devices include but are not limited to, desktops, laptops, tablets, and mobile phones.

Hardening

Kantar has established hardening standards and configuration baselines in-line with industry best practice. This includes but is not limited to, workstations, virtual machines (VMs), and cloud containers. Endpoint devices must be hardened and securely configured in accordance with Kantar's baseline security standards. These include, but are not limited to, running approved operating systems disabling insecure features and receiving updates through a centralised enforcement method.

All desktops and laptops have host-based firewall configured to control inbound network traffic and have full hard drive encryption in place using industry standard tools. An automatic device lockout after 5 failed authentication attempts and a screen lock after 15 minutes of inactivity is enforced by a configuration policy. USB ports on endpoints are disabled, and security event logging is in place.

Malware Defence

Kantar deploys anti-malware and endpoint detection and response (EDR) solutions which are maintained on all endpoint devices. EDR monitors for sign of malicious behaviour and takes pre-defined protection steps to protect the endpoint and wider network.

Mobile Application Management

Kantar uses MAM & MDM (Mobile Application/Device Management) capabilities within Microsoft 365 to manage mobile devices, both company supplied and BYOD.

9. Vulnerability Management

Vulnerability Scanning & Management

All endpoints undergo vulnerability scanning and remediation in-line with Kantar's Vulnerability Management Standard. This scanning is conducted in real time, assesses, and discovers known or new vulnerabilities. All infrastructure is regularly scanned using automated network or agent vulnerability scanning tools. Kantar actively manages its perimeter and scans for vulnerabilities on public facing assets, daily.

Patching

Security patches are applied in a regular and timely manner in-line with the risk they pose to the organisation with change control in place. Operating system patches are addressed throughout the organisation on a monthly schedule by the service provider beginning the weekend after Patch Tuesday by Microsoft. Zero-day vulnerabilities are patched ad-hoc as needed and the rollout is managed as an incident where relevant.

Penetration Testing

Kantar conducts regular penetration tests against critical applications and infrastructure using a combination of internal expertise and external CREST certified third party resources.

10. Data Security

Kantar is committed to the responsible collection, management, use and protection of data, recognising its obligations to all stakeholders and complying with applicable Data Privacy Regulations.

Data Classification and Handling

Kantar's Data Classification and Handling Guidance is owned by Global Compliance and defines levels of data classification (Public, General, Confidential, Restricted) and defines relevant handling requirements such as data transfer, storage, retention, and disposal.

Data Backup Principles

Data backups are captured according to prescribed backup schedules appropriate to each application or instance. All backup data is classified, stored using industry best practice encryption standards and retained as per Kantar's Data Classification and Handling policy.

Data Security Controls

Kantar implements controls designed to safeguard information from unauthorised access and compromise. Data in transit is encrypted using secure file transfer systems, including SFTP and the application of TLS encryption of email.

Endpoint devices are secured with full disk encryption. Where encryption of data at rest is applied, components are configured to support the strongest cipher suites possible. Keys must be distributed and stored in a secure environment, such as designated key management systems and maintained for the lifecycle of the data.

Data Loss Prevention (DLP)

Kantar has implemented the use of sensitivity labels for email and file classification. Kantar has processes in place to identify, monitor and address risks resulting from non-compliance with data classification and handling practices. Kantar has implemented technical controls such as USB port write blocking and sensitivity labelling. The use of removable media with workstations is disabled by default. URL content filtering methods include controlling access to websites based on URL categories.

Data Privacy

Kantar is committed to the secure, legal, and ethical processing of data, including the personal data we hold about our research, survey subjects, panellists, staff, clients, and suppliers. To protect individuals' privacy rights, Kantar's Privacy and Compliance functions have established a global framework for managing Personal Data that incorporates obligations required for applicable Data Privacy Regulations.

The Kantar Data Protection Framework outlines Kantar's obligations in relation to:

- Data processing activities and data inventory
- Data Protection impact assessments
- The rights of individuals
- Privacy notices
- Lawful collection and use of Personal Data
- Sensitive and children's data
- Data minimization
- International transfers
- Data classification and handling
- Data incidents
- Third parties

11. Personnel Security

Kantar ensures all personnel have relevant security checks/screening in place, appropriate for their role, the data to which they have access and the market in which they operate.

12. Physical Security

Kantar has documented and implemented a Physical Security Statement applicable to all Kantar facilities. This includes, but is not limited to, surveillance measures including anti-tail gating, access control, CCTV, alarm systems and sign in/sign out procedures. The Physical Security Statement is reviewed regularly.

13. Supplier Security

Kantar's Supplier Security Standard details the security activities which need to accompany the use of outsourced services. Where suppliers have been selected to work with Kantar, supplier contracts must contain appropriate and necessary confidentiality provisions. The assessment of third parties prior to their formal engagement by Kantar must include a review of their criticality to Kantar and maturity of their information security capabilities, ensuring they are in-line with Kantar security standards. The ongoing information security capability of contracted third-party organisation shall be periodically re-assessed by Kantar to ensure that the criticality of a supplier has not changed, and no new risks have been introduced.

14. Cyber Threat Intelligence (CTI)

Kantar's CTI team utilizes a SaaS-based Threat Intelligence Platform from a third party to inform the alerting and reporting of these services. CTI also utilize open-source intelligence findings and incorporate known threats and threat actors from historical incidents. On an operational basis, CTI provides the following services to internal stakeholders: Deep/Dark Web Monitoring, Vulnerability Intelligence, Major Incident Response, Support, Threat Landscape Reporting and Metrics.

15. Logging and Monitoring

Kantar's Log Management Standard defines logging requirements such as access, events, sources, and levels of appropriate activity detail. System and audit logs must be retained across enterprise assets for a minimum of 90 days with the ability to archive for a longer duration. All relevant logs are sent to a centralised log infrastructure/SIEM or syslog. Kantar Security Operations ensures that logs are continuously monitored and reviewed by personnel from the Kantar Security Operations Centre (SOC) to detect anomalous events and apply resolutions in a timely manner.

16. Cyber Incident Response

Kantar's Cyber Incident Response Management Framework enables effective detection and planning responses to contain the potential impact on Kantar's information and technology environment. This framework is used by Kantar's Cyber Security Incident Response Team (CSIRT) and provides guidance for preparation, detection, analysis, notification & escalation, containment, eradication, recovery, and post incident reviews as per industry best practice. Mechanisms for detection and reporting of security incidents have been implemented within the organisation and feed into the Crisis Management Framework as needed. As part of the continual improvement of Kantar's Cyber Incident Response Capability, tabletop exercises are performed.

17. Business Continuity and Disaster Recovery

Kantar requires all divisions and business areas to maintain and implement Business Continuity Plans (BCPs) covering crisis management, continuity of critical services, and recovery activities. The Technology platform groups responsible for maintaining the applications and systems must ensure Disaster Recovery procedures are defined. Infrastructure resiliency is in place to meet the requirements of the business. BCP and DR documentation must be reviewed and tested at least annually.

18. Artificial Intelligence (AI)

Kantar is committed to responsibly leveraging artificial intelligence to enhance its services while maintaining strong safeguards around safety, compliance, and resilience. Through continuous monitoring and alignment with evolving regulations, Kantar ensures that AI is used in a way that protects the integrity of its systems, data, and services. Kantar has a suite of IT security policies and controls that are divided into several key areas, data encryption, infrastructure security, and identity governance. These controls are reinforced by risk reviews, including privacy, security, and EU AI Act evaluations. All users are guided by Kantar's AI Responsible Use Policy to ensure secure and compliant use. More details can be found in the Kantar AI Explainability Statements.

ANNEX IV

ROLES OF THE PARTIES

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. In summary:

- If Kantar provides the relevant Services using its own survey respondents, data, or data or survey respondents obtained from third parties, then if any of that data is Personal Data Kantar shall act as an independent Controller. To the extent that the Client receives (or is made available) any Personal Data from Kantar, the Client shall also act as an independent Controller
- If Kantar provides the relevant Services using survey respondents obtained or sourced by the Client, then, with regard to the Processing of Personal Data, the Client is the Controller, Kantar is a Processor on behalf of the Client

In further detail, the Parties agree the following determinations as to their roles as either a Controller or Processer of Personal Data regarding the envisaged Services:

1. CLIENT AS INDEPENDENT DATA CONTROLLER AND KANTAR AS INDEPENDENT DATA CONTROLLER:

(a) ***Traditional market research, qualitative or quantitative (panel or business intelligence report).*** *Kantar is fully and solely responsible for the recruitment of survey respondents, and collection and management of their answers/inputs.*

Recruitment. *Kantar either recruits new respondents or reaches out to the respondents that it already has in its respondent database, or elsewhere, at its discretion.*

Questionnaire. *Kantar then, using its professional discretion and expertise, designs and agrees the questionnaire with the Client, and the Client may provide content for testing. Kantar sends the questionnaire and tested content to the respondents through an online "community" platform, owned and controlled or commissioned by Kantar.*

Reporting. *Kantar is fully responsible for analysing collected answers/inputs and reporting the results/outcome. Kantar does not provide any Personal Data of the respondents to the Client in its reports. Typically, the Client neither collects, nor has access to any Personal Data of respondents at any time. If the Client requires access to Personal Data, a separate consent must be obtained for this transfer of Personal Data, which shall include the Client's transparency information, such as its privacy notice.*

Ongoing use of Personal Data. *Where Kantar has obtained Personal Data outside of Client's database it will be free to use the Personal Data for other clients.*

(b) ***Syndicated market research.*** *Kantar may provide the Services using other data sources, at its sole discretion. Some of those Services may include datasets that are "syndicated", meaning that they are sold or licensed to Kantar's other clients. In such cases, Kantar is fully and solely responsible for the sourcing, collecting, storage, analysis, delivery, formatting of that data (including any Personal Data), and is free to use it for other clients. It is not anticipated that the Client will receive, nor have access to, any Personal Data as a result of these Services.*

2. CLIENT IS A DATA CONTROLLER AND KANTAR IS A DATA PROCESSOR OF CLIENT PERSONAL DATA:

(a) ***Client-supplied sample market research, qualitative or quantitative (i.e. Customer Experience (CX) or Compass services).*** *The client is responsible for the recruitment of survey respondents, and (to safeguard the data of its customers, or otherwise) provides Kantar with specific instructions about the processing of the personal data.*

Recruitment. *Kantar obtains the details of survey respondents from the Client, for example, from Client's consumer, customer or employee database. Kantar is only provided with the details of enough respondents (this may sometimes include a margin in case some respondents do not participate) to complete the survey.*

Questionnaire. *Kantar then agrees the questionnaire and any tested content with the Client. Kantar sends the questionnaire and any tested content to the respondents and conducts research, or Kantar sends the questionnaire and any tested content to the respondents through an online "community" platform, owned and controlled or commissioned by Kantar.*

Reporting. *Kantar reports back to the Client aggregated data of respondents' answers/inputs. Kantar does not provide any Personal Data of the respondents to the Client in its reports. OR Kantar may provide access to the platform, where the Client will be able to view videos, pictures, or answers of the respondents (but no other Personal Data of the respondents) in its reports to illustrate the findings of the research.*

Ongoing use of Personal Data. *In each case Kantar uses the Personal Data only for the purposes of providing the Services.*

(b) ***Online video interviews****. The same description applies as described above at 2(a), however the market research involves the Client providing content to Kantar for testing and discussing with the respondents. In some instances, the Client may use their own separate third-party supplier for interviewing respondents, but Kantar may be asked to analyse collected answers/inputs and report the results/outcome to the Client. The Client may also listen to the video interviews. Kantar uses the Client Personal Data only for the purposes of providing the Services.*