KANTAR

KANTAR AND SUPPLIER DATA PROTECTION AGREEMENT

This Data Protection Agreement (**DPA**) will be effective on and from the date the Parties execute, or executed, the Main Agreement described below (**Effective Date**).

BACKGROUND

(A) This DPA is written on the basis that on the Effective Date the Supplier and Kantar (together the **Parties**) will either enter into an agreement for services provided by the Supplier to Kantar that involve the processing of Personal Data or that the Parties have already entered into one or more of these agreements and they wish to supplement and/or amend that agreement or agreements.

(B) In this DPA the term **Main Agreement** refers to each agreement made between the Parties as referred to in paragraph A individually, and if the Main Agreement is a framework a reference to a Main Agreement includes call-off contracts or SOWs made under it.

(C) The Parties agree that these DPA terms form part of their Main Agreement(s) and related SOWs and will supplement and/or amend existing privacy and data protection terms contained in it or them, and that if there is a conflict with existing or other terms this DPA shall prevail to the extent set out below.

NOW, THEREFORE, the Parties agree as follows:

1. **DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning and interpretations given to them in the Main Agreement. In this DPA, the following terms shall have the meanings and interpretations 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 Supplier, any entity which is Controlled by Supplier (and **Supplier Affiliate** shall be construed accordingly).

1.2 **Kantar Personal Data** means any Personal Data Processed under the Main Agreement by Supplier or a Sub-processor (either as an independent Controller or as a Processor on behalf of Kantar) whether Kantar is a Controller or is itself acting as a Processor for one of Kantar's end client(s).

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 **Data Processing Particulars** means the description of Processing of Kantar Personal Data, as set out within the Main Agreement (or relevant SOW) carried out in connection with the provision of Services under that Main Agreement (or relevant SOW).

1.5 **Data Protection Laws** means EU Data Protection Laws and UK Data Protection Laws together with any equivalent legislation and all other Applicable Laws and regulations in any relevant jurisdiction relating to the Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by a relevant regulator or Supervisory Authority in relation to such Applicable Laws, in each case as amended, repealed or replaced from time to time.

1.6 **EU Data Protection Laws** means the EU GDPR and laws implementing or supplementing the EU GDPR, the Privacy and Electronic Communications Directive 2002/58/EC and any other Applicable Laws relating to the Processing of Personal Data and privacy, including any applicable delegated acts adopted by the European Commission and any applicable national legislation made under or otherwise adopted by Member States of the European Economic Area pursuant to specific rights or powers contained within the EU GDPR.

1.7 **EU GDPR** means EU 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.

1.8 **Independent Auditor** means an auditor from PwC, Deloitte, KPMG or EY (Ernst & Young) or another mutually agreeable internationally recognized auditing firm that is not employed on a contingency fee basis.

1.9 **Personnel** means either Party's stakeholders, directors, employees, agents, consultants, subcontractors, or other persons authorized by (i) either Party (ii) their Affiliates (iii) their subcontractors engaged in the provision of Services.

1.10 **Restricted International Transfer** means a transfer of personal data from a party established in: (i) a country that is deemed adequate (by the European Commission or any other competent body for the purposes of Data Protection Laws) to a Third Country, (ii) from any Third Country to another Third Country.

1.11 **Restricted International Transfer Agreement** means the relevant standard contractual clauses (such as the Standard Contractual Clauses or the UK International Data Transfer Agreement) or any other standard or non-standard contractual clauses required under Data Protection Laws (as amended or replaced from time to time).

1.12 **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.

1.13 **Standard Contractual Clauses** means the standard contractual clauses (adopting the appropriate module that reflects the relationship of the Parties) approved by European Commission decision 2021/915 on standard contractual clauses for the transfer of Personal Data to processors established in Third Countries, as amended or replaced from time to time.

1.14 **Subcontractor** means any third party (excluding any Supplier Affiliate) to whom Supplier has delegated any function or obligation to provide the Services.

1.15 **Sub-processor** means any Subcontractor appointed by Supplier as set out in Clause 6 (Sub-processors) to Process Kantar Personal Data on behalf of Kantar in connection with the Main Agreement.

1.16 **UK Addendum** means a separate UK addendum to be used in conjunction with the Standard Contractual Clauses if there is a Restricted International Transfer under Standard Contractual Clauses that also includes the UK.

1.17 **UK Data Protection Laws** means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in the United Kingdom in each case as amended, repealed or replaced from time to time.

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

1.19 **UK International Data Transfer Agreement** or **UK IDTA** means the Restricted International Transfer Agreement required for new Processing arrangements entered into from 21 March 2024 for the transfer of Personal Data from the UK to processors established in Third Countries (as amended or replaced from time to time).

1.20 The terms, **Binding Corporate Rules Commission, Controller, Data Subject, Member State, Personal Data, Processing, Processor, Third Country** and **Supervisory Authority** shall have the same meaning as in Data Protection Laws, and their cognate terms shall be construed accordingly.

1.21 For the purposes of this DPA:

1.21.1 any reference to Parties shall be to Kantar, Supplier and the relevant parties to the relevant SOW (and Party shall mean any one of them);

1.21.2 any references to Kantar shall mean Kantar and the relevant Kantar Affiliate that is a party to that SOW; and

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

2. SUPPLIER PROCESSING AS AN INDEPENDENT CONTROLLER

2.1 The parties acknowledge that with regard to the Kantar Personal Data, Supplier may act as an independent Controller, and if acting as an independent Controller, the Supplier shall conduct the Processing of Kantar Personal Data as follows:

2.1.1 all Processing shall be carried out in accordance with Data Protection Laws;

2.1.2 Kantar Personal Data shall be treated as Confidential Information (as defined in the Main Agreement);

2.1.3 Processing shall be for the purposes of providing the Services only.

2.2 To the extent that Supplier acts as an independent Controller, Clause 3 (Supplier Processing as a Processor) to Clause 12 (Restricted International Transfers and Processing in Third Countries) (inclusive) of this DPA shall not apply unless this Clause 2 states otherwise.

2.3 Kantar confirms that it has and will fulfil its obligations required under the Data Protection Laws, that it has the authority to provide Kantar Personal Data to the Supplier in connection with the Services and that at the time when any Kantar Personal Data is provided to the Supplier it has been Processed by Kantar in accordance with the Data Protection Laws.

2.4 Where the Supplier acts as an independent Controller, the Parties agree that the following clauses shall apply:

2.4.1 Clause 4 (Technical and organisational measures);

2.4.2 Clause 5 (Rights of Data Subjects); and

2.4.3 Clause 8 (Data Incident Management Notification).

2.5 Supplier warrants that any Restricted International Transfers are subject to Clause 12 (Restricted International Transfers and Processing in Third Countries).

2.6 Upon request, each party shall provide the other with information relating to its Processing of the Kantar Personal Data as reasonably required for the other to satisfy its obligations under Data Protection Laws.

3. SUPPLIER PROCESSING AS A PROCESSOR

3.1 The parties acknowledge that with regard to the Kantar Personal Data, Supplier may act as a Processor of Kantar Personal Data and agree that the terms of Clause 3 (Supplier Processing as a Processor) to Clause 12 (Restricted International Transfers and Processing in Third Countries) (inclusive) shall apply.

3.2 Supplier shall Process Kantar Personal Data on behalf of Kantar in compliance with Kantar's lawful instructions for the purposes described in the Data Processing Particulars (**Permitted Purposes**). The Data Processing Particulars shall be completed with the relevant SOW under which Supplier is required to process Kantar Personal Data in the provision of the Services.

3.3 If other Processing is required by local applicable law (including local laws in the relevant Sub-processor's country), Supplier shall inform Kantar of that legal requirement before such Processing, unless that local law prohibits this on important grounds of public interest. Notwithstanding the foregoing, Supplier shall not carry out such other Processing (including transfer of Kantar Personal Data to a public authority) unless there is a legal mandate between the Kantar country and the relevant local country for Supplier to carry out such Processing, and any transfer shall be carried out in accordance with Annex 1 of this DPA.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 Supplier shall provide and maintain appropriate technical and organisational measures that are commensurate with the nature of the Services (including, as a minimum, the technical and organisational security measures set out in or annexed to the Main Agreement (and/or the relevant SOW) (the **TOMs**)).

4.2 Supplier agrees that it shall ensure that any changes made to the technical and organisational measures will result in a level of protection for the Kantar Personal Data that is the same as, or greater than, that which applied as at the at the Effective Date.

4.3 Supplier shall:

4.3.1 only involve Supplier Personnel to Process Kantar Personal Data under the Main Agreement who have had appropriate training on the care and handling of Personal Data;

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

4.3.3 ensure the reliability of Supplier Personnel to whom Supplier has provided access to Kantar Personal Data.

4.4 Kantar shall comply with and will continue to comply with Data Protection Laws and Supplier shall inform Kantar if, in the Supplier's opinion, instructions given by Kantar infringe Data Protection Laws.

5. RIGHTS OF DATA SUBJECTS

5.1 Supplier shall to the extent legally permitted, immediately notify Kantar if Supplier 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 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 (each a **Data Subject Request**).

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

5.3 If Kantar does not have the ability to address a Data Subject Request, Supplier shall upon Kantar's request provide commercially reasonable efforts to assist Kantar in responding to such Data Subject Request, to the extent Supplier is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

5.4 If the Supplier is acting as a Processor, then neither Supplier nor relevant Sub-processor shall respond to a Data Subject Request unless authorized to do so by Kantar.

6. SUB-PROCESSORS

6.1 Supplier will not share, transfer, disclose, make available or otherwise provide access to any Kantar Personal Data to any third party (including Supplier Affiliates), or contract any of its rights or obligations concerning Kantar Personal Data performed on behalf of Kantar pursuant to this DPA to a Sub-processor without the specific written consent of Kantar. For the avoidance of doubt, Kantar's prior written consent must be obtained for each and any change of Sub-processor no later than 60 calendar days prior to such change.

6.2 Supplier represents and warrants that such Sub-processor has entered into binding written agreements with the Supplier that are substantially the same and no less onerous as those imposed on the Supplier pursuant to this DPA.

6.3 Supplier shall provide Kantar with the necessary information to help it verify the Sub-processor's compliance with its data protection obligations pursuant to this DPA and Data Protection Laws.

6.4 Supplier shall remain fully liable towards Kantar for the performance of any and all Sub-processors obligations under this DPA and all Data Protection Laws.

7. AUDIT

7.1 In addition to any audit rights within the Main Agreement and upon request by Kantar, Supplier allows Kantar (either on its own or on behalf of its end client(s) as Controller) or an Independent Auditor instructed by Kantar to audit and review the Supplier, and the Sub-processor's, information security program, data processing facilities and data protection compliance program in order to verify compliance with this DPA, Data Protection Laws and Kantar or Kantar's own obligations to its end client(s) (**Data Protection and Security Audit**).

7.2 Such Data Protection and Security Audit may include tests designed to breach the Supplier's, or Sub-processor's, information security program and associated security measures (including security penetration testing) and shall be conducted with no less than 10 days' prior written notice.

7.3 If Kantar reasonably believes that the results of a Data Protection and Security Audit identifies a weakness in the security measures adopted by the Supplier, or any Sub-processor(s), the Supplier shall evaluate such weakness and provide a suitable solution to Kantar (or its end client's(s')) satisfaction within timescales agreed by Kantar.

7.4 The Supplier acknowledges that any regulator or its agent may from time to time audit the Supplier, or any approved Sub-processors, and that any such audit shall not be subject to any of the restrictions set out in this Clause 7.

7.5 The Supplier shall maintain a record of its Processing activities conducted for and on behalf of Kantar. This record shall be made available to Kantar within 48 hours of Kantar making a request.

8. DATA INCIDENT MANAGEMENT AND NOTIFICATION

8.1 In addition to compliance with the relevant technical and organizational measures, Supplier will maintain security incident management policies and procedures and shall notify Kantar without undue delay (and in any event within 36 hours) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Kantar Personal Data, transmitted, stored or otherwise Processed by Supplier or its Sub-processors which results in any actual loss or misuse of Kantar Personal Data (a **Data Incident**).

8.2 Supplier shall provide Kantar with sufficient information to allow Kantar to meet any obligations to assess and report a Data Incident under the Data Protection Laws, which may be provided in stages as it becomes available to Supplier and shall include the following:

- 8.2.1 a description of the nature of the Data Incident, including details of any Sub-processors involved, the categories and numbers of Data Subjects concerned, and the categories and numbers of Kantar Personal Data records concerned;
- 8.2.2 the name and contact details of Supplier's or the relevant Supplier Affiliate's data protection officer or other relevant contact from whom more information may be obtained;
- 8.2.3 the likely consequences of the Data Incident; and
- 8.2.4 the measures taken or proposed to be taken to address the Data Incident.

8.3 Supplier shall make all 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 the Data Incident to the extent that the remediation is within Supplier's reasonable control.

8.4 Supplier shall be liable for all costs arising from a Data Incident caused by a breach of this Clause 8.

8.5 Where the Supplier is acting as a Processor, in the event of a Data Incident, Kantar (subject to any obligations Kantar has to its end client(s)) shall be responsible for notifying Data Subjects and / or Supervisory Authorities. Before any such notification is made, Kantar shall, where possible, consult with and provide Supplier an opportunity to comment on any notification made in connection with a Data Incident.

9. RETURN AND DELETION OF KANTAR PERSONAL DATA

Supplier shall, and shall procure that Sub-processors shall, at any time on Kantar's request, delete or return all Kantar Personal Data except that this requirement shall not apply to the extent that: (i) Supplier or Sub-processors are required to retain Kantar Personal Data for compliance with applicable laws or regulatory requirements; (ii) Kantar 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.

10. 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.

11. **DATA PROTECTION IMPACT ASSESSMENT**

11.1 Upon Kantar's request, Supplier shall, and shall procure that Sub-processors shall, provide Kantar with reasonable cooperation and assistance, at Kantar's cost, needed to fulfil Kantar's obligation to carry out a data protection impact assessment (**DPIA**) including but not limited to where a type of Processing is likely to result in a high risk to the rights and freedoms of Data Subjects, to allow Kantar to comply with its obligations as a Controller in relation to data security, DPIA and any related consultations under Data Protection Laws.

11.2 The Supplier and each Sub-processor shall comply with its obligation to consult the relevant Supervisory Authority prior to Processing where a DPIA indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

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

12.1 Supplier represents and warrants that it has entered into relevant Restricted International Transfer Agreements with its Sub-processors in respect to any Restricted International Transfers, or that Restricted International Transfers will be covered at the time of the transfer by Binding Corporate Rules.

12.2 The Restricted International Transfer Agreement terms shall be 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 options for the Standard Contractual Clauses (or equivalent options) are set out in paragraph 1 (Options (from EU SCCs) and equivalent terms) in Annex 1.

12.3.2 the Parties shall cooperate with each other to carry out the Supplementary Security Measures set out in paragraph 2 (Supplementary Security Measures) of Annex 1.

13. **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.

KANTAR

ANNEX 1

RESTRICTED INTERNATIONAL TRANSFER AGREEMENT TEMPLATES

(Provided for reference)

UK International Data Transfer Agreement

https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx

UK Addendum

https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

Module: (1) EU Controller to Controller | (2) Controller to Processor | (3) Processor to Processor | (4)Processor to Controller Restricted International Transfer Agreement

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

1. Options (from EU SCCs) and equivalent terms

1.1 The Parties hereby make the following options (from the Standard Contractual Clauses) which shall apply in each Restricted International Transfer Agreement entered into by the Parties.

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

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

1.4 **Clause 13(a) (Supervision)** means the Supervisory Authority in the Data Exporter country.

1.5 **Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction)**. Option 2 shall apply. The governing law and courts in the Data Exporter country shall apply.

1.6 **Annex I** of the Restricted International Transfer Agreements shall be deemed to be pre-populated with the relevant sections of Data Processing Particulars.

1.7 **Annex II** of the Restricted International Transfer Agreements shall be deemed to be pre-populated with the relevant TOMs.

1.8 **Annex III** of the relevant Restricted International Transfer Agreement Module shall be deemed to be pre-populated with the details of the Parties in the Main Agreement or in the relevant Sub-processing agreement. The relevant Module is set out in the relevant Dara Processing Particulars.

2. 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 Kantar Personal Data or surveillance order (**Order**).

2.2 Supplier / Sub-processor in a Third Country shall notify Kantar without undue delay of any Order.

2.3 Supplier / Sub-processor will not attempt to respond in detail to such a request without the relevant Controller's prior written consent. Supplier / Sub-processor may, however, provide generic information (not including Kantar Personal Data) to public / private / regulatory authority as part of its obligations to cooperate without consulting or obtaining the prior consent of the relevant Controller.

2.4 If the Parties establish that there is a legal basis to comply with the Order, the Parties shall arrange for the Supplier / Sub-processor to provide information they have resolved to provide.

2.5 The Parties shall:

- 2.5.1 assist Data Subjects in exercising their rights in connection an Order
- 2.5.2 cooperate to notify relevant Data Subjects and assist Data Subjects in exercising their rights in connection with the Order by email prior to disclosing the content of the Order to them, however the Data Subject will not be notified if the Order legally prohibits Supplier / Sub-processor from doing so, or if there is an emergency
- 2.5.3 in any case notify the Data Subject as soon as it is legally permitted to do so or when the emergency (if any) has passed.

2.6 Supplier / Sub-processor shall:

- 2.5.4 not without notifying Kantar beforehand, create back doors or similar programming in its systems (used for Processing Kantar Personal Data), that could be used by public / private / regulatory authorities to access Kantar Personal Data and Supplier / Sub-processor will provide certification that it has not purposefully created such access to Kantar Personal Data
- 2.5.5 not purposefully create or change its business Processes in a manner that facilitates access to Kantar Personal Data
- 2.5.6 promptly inform Kantar of any change in local law that requires Supplier / Sub-processor to comply with Orders that negatively affect the security of Kantar Personal Data
- 2.5.7 in accordance with clause 7 (Audit) permit Kantar (or its end client(s) as Controller) to conduct an audit or inspection of the relevant Processing facilities to verify if unauthorized transfers of Kantar Personal Data have been made to public / private / regulatory authorities
- 2.5.8 regularly publish a cryptographically signed message informing Kantar that as of a certain date and time it has received no Order. The absence of an update of this notification will indicate to Kantar that the Supplier / Sub-processor may have received an Order in which case Kantar may suspend Processing activities until the Supplier / Sub-processor has complied with its obligations in this clause. Supplier shall be liable to the Kantar for Supplier / Sub-processor's failure to meet its Processing obligations as a result of such failure.