Attest

Data Processing Agreement

This Data Processing Agreement and its Annexes ("**DPA**") form part of the Agreement entered into by Customer (as defined at Annex I) and Attest Technologies Limited ("**Attest**") and sets out the way in which personal data shall be processed under the Agreement. Any capitalised terms used but not defined in this DPA shall have the meaning set out in the Agreement. This DPA is entered into on the day that the Agreement is signed by and between Customer and Attest. In the event of conflict between the terms of the Agreement and the terms of the DPA, the terms of the DPA shall prevail.

1. In this DPA, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in EU/UK Data Protection Law;

(b) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law;

(c) "**EU/UK Data Protection Law**" means: (i) 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 (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

(d) **"Respondent Unique ID"** means a pseudonymised identifier created by the Customer for use in connection with Attest's Unique ID functionality ("**Unique IDs**"), such identifier having been designed by the Customer to be used in place of an identifier that could be more easily linked to an individual (such as a name or email address).

(e) **"Respondent Personal Data"** means respondent personal data that is collected, processed, or transferred by and/or to the Customer through the Attest Service, in accordance with paragraph 4 of Attest's Acceptable Use Policy. This personal data is currently limited to video images and audio data of respondents collected through Video Responses, and the Respondent Unique IDs and demographic data that is used in connection with Unique IDs.

(f) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(g) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

2. *Relationship of the parties:* In respect of Respondent Personal Data, the Customer shall be the

controller and Attest shall be a processor. Each party shall comply with all obligations that apply to it under Applicable Data Protection Law.

3. *Prohibited data:* The Parties agree that the Attest Service is not intended for the processing of special category or sensitive data, or any personal data other than Respondent Personal Data. The Customer shall not ask any survey respondents to share any personal data other than Respondent Personal Data, or any special category or sensitive data.

4. *Purpose limitation:* Attest shall process Respondent Personal Data for the purposes described in Annex I and strictly in accordance with the documented instructions of the Customer as set out in in Annex I (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law. In no event shall Attest process Respondent Personal Data for its own purposes or those of any third party or sell or share Respondent Personal Data. Attest shall immediately inform the Customer if it becomes aware that such processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor the Customer's compliance with Applicable Data Protection Law).

5. *Restricted transfers:* The parties agree that when Respondent Personal Data that is collected, processed, or transferred by and/or to the Customer is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

5.1. in relation to Respondent Personal Data that is protected by the EU GDPR, the EU SCCs will apply where there is a Restricted Transfer from Attest to Customer, and shall be completed as follows:

5.1.1. Attest shall be the “data exporter” and Customer shall be the “data importer”;

5.1.2. Module 4 (Processor to Controller) shall apply;

5.1.3. in Clause 7, the optional docking clause will apply;

5.1.4. in Clause 17, the EU SCCs will be governed by Irish law;

5.1.5. in Clause 18, disputes shall be resolved before the courts of Ireland;

5.1.6. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to these Terms; and

5.1.7. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to these Terms.

6. *Onward transfers:* Attest shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Respondent Personal Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law and pursuant to either Standard Contractual Clauses implemented between the relevant exporter and importer of the Respondent Personal Data, or another appropriate mechanism. In the event that any provision of the Agreement contradicts, directly or indirectly, the Standard Contractual Clauses or this DPA, the Standard Contractual Clauses shall prevail, followed by this DPA, then the Agreement (save where the Agreement explicitly states otherwise).

7. *Confidentiality of processing:* Attest shall ensure that any person that it authorises to process the Respondent Personal Data (including Attest's staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Respondent Personal Data who is not under such a duty of confidentiality. Attest shall ensure that all Authorised Persons process the Respondent Personal Data only as necessary for the Permitted Purpose.

8. *Security:* Attest shall implement appropriate technical and organisational measures to protect the Respondent Personal Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**"), and agrees that it shall as a minimum maintain the technical and organisational measures which are set out at Annex II. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity

for the rights and freedoms of natural persons.

9. *Subprocessing:* The Customer consents to Attest engaging third party subprocessors to process the Respondent Personal Data provided that: (i) Attest provides prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform), which may be given by posting details of such addition or removal at the following URL: https://www.askattest.com/legal/privacy-policy; (ii) Attest imposes data protection terms on any subprocessor it appoints that protect the Respondent Personal Data, in substance, to the same standard provided for by this DPA and grant the Customer, as a third party beneficiary, the right to terminate the subcontract and to instruct the subprocessor to erase or return the Respondent Personal Data in the event that Attest has factually disappeared, ceased to exist in law or has become insolvent; and (iii) Attest remains fully liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor.

10. *Cooperation and data subjects' rights:* Attest shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to the Customer at its own expense to enable the Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Respondent Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Attest, Attest shall promptly inform the Customer providing full details of the same.

11. *Data Protection Impact Assessment:* Attest shall provide the Customer with all such reasonable and timely assistance as the Customer may require in order to enable it to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist the Customer to consult with its relevant data protection authority.

12. *Security incidents:* Upon becoming aware of a Security Incident, Attest shall inform the Customer without undue delay (and, in any event, within 72 hours) and shall provide all such timely information and cooperation as the Customer may require in order for the Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Attest shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep the Customer informed of all developments in connection with the Security Incident.

13. *Deletion or return of Data:* Upon termination or expiry of the Agreement, Attest shall (at the Customer's election) destroy or return to the Customer all Respondent Personal Data (including all copies of the Respondent Personal Data) in its possession or control (including any Respondent Personal Data subcontracted to a third party for processing). This requirement shall not apply to the extent that Attest is required by any Applicable Data Protection Law to retain some or all of the Respondent Personal Data, in which event Attest shall isolate and protect the Respondent Personal Data from any further processing except to the extent required by such law until deletion is possible.

Annex I

Data Processing Description

This Annex I forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Customer

1.	Name:	The Customer's name as set out in the Customer's Order Form.
	Address:	The Customer's registered address as set out in the Customer's Order Form.
	Contact person's name, position and contact details:	As set out on the Order Form.
	Activities relevant to the data transferred under these Clauses:	The provision of the Attest Services by Attest to the Customer.
	Signature and date:	This Data Processing Agreement shall be deemed executed on the date this Agreement has been signed by both parties.
	Role (controller/processor):	Controller of Respondent Personal Data.

Attest

1.	Name:	Attest as described in the Agreement.
	Address:	Attest's address as specified in the Agreement.
	Contact person's name, position and contact details:	Legal Team legal@askattest.com
	Activities relevant to the data transferred under these Clauses:	The provision of the Attest Services by Attest to the Customer.
	Signature and date:	This Data Processing Agreement shall be deemed executed on the date this Agreement has been signed by both parties.
	Role (controller/processor):	Processor in respect of Respondent Personal Data.

B. DESCRIPTION OF PROCESSING

Categories of data subjects whose personal data is processed and/or transferred:	Respondents taking part in Video Response and/or Unique ID surveys on the Attest Platform.
Categories of personal data:	• Respondents taking part in Video Response surveys: Video images and audio of respondents. • Respondents who have been assigned a Respondent Unique ID within the Attest platform: the unique identifier that is assigned to the Own Audience Respondent by the Customer and any demographic data shared in relation to that individual.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	None.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Agreement.
Nature of the processing:	Processing by Attest for the provision of the Attest Service to the Customer pursuant to the Agreement.
Purpose(s) of any data transfer and further processing:	Attest will process and transfer this data in order to facilitate the market research requested by Customer, and provide access to the results of that research.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	For the duration of the Agreement.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	N/A.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	Where the EU GDPR applies, the competent supervisory authority shall be determined in accordance with Clause 13 of the EU SCCs. Where the UK GDPR applies, the UK Information Commissioner's Office.

Annex II

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of encryption of data	All data is encrypted at rest. We use industry standard AES-256 encryption. All data in transit is encrypted using TLS 1.2. All of our web applications enforce the use of HTTPS. All database data and backups are encrypted.
Measures for ensuring physical security of locations at which personal data are processed	Our technical infrastructure, including databases, is hosted on Amazon Web Services ('AWS'), which means we inherit the robust security structure and mechanisms that are maintained by AWS. You can read about AWS compliance at https://aws.amazon.com/compliance/programs/.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems, data and services and managing incidents	All Attest employees and contractors are required to sign standardised employment or contractor agreements prior to their start date, which contain detailed confidentiality provisions. All Attest employees complete mandatory training, including data protection and cybersecurity training. Our databases are backed up daily and stored for two weeks. Our Kafka cluster is backed up to Amazon S3 as soon as new data is available. We have a documented incident response plan that would be followed in the case of a technical incident, which ensures that a team involving both a legal representative and customer representative are involved from the beginning to manage communications and notifications. Where the issue is one that may have an impact on customers, customers would be notified.

Measures for user identification and authorisation	Customers: Users are authenticated via username and password combination. These are checked against our own credential store which is stored in our database. We have applied a secure password policy for our customers, which is in accordance with the National Institute of Standards and Technology (NIST) and any new passwords are automatically cross-checked against a database of compromised passwords before they're accepted. Customers are also able to set up 2-step verification on their accounts: https://intercom.help/attest/en/articles/4859091-log-in-and-2-step-verification. Attest Employees: All systems used by Attest employees are configured with SAML login where permitted, backed by their email account which is subject to strict password content and re-set policies. Access to all systems and email accounts are removed on the employee's final working day. .
Measures for the protection of data during transmission	All data in transit is encrypted using Transport Layer Security (TLS 1.2).
Measures for the protection of data during storage	Data is stored in our database services which are managed by AWS and located in Dublin, Ireland. Data storage on local machines is not permitted.
Measures for ensuring system configuration, including default configuration	Attest has in place an Access Control Policy which stipulates access controls, including system configuration.
Measures for internal IT and IT security governance and management	Attest has an IT Security Policy and related documentation which is managed by our IT Manager and Legal Team.
Measures for ensuring data minimisation	Attest only collects the minimum personal data required for the purpose of the processing. Attest also completes detailed reviews of any new suppliers and/or any processing activities by third parties to ensure that only minimal data is processed.
Measures for ensuring accountability	Data protection impact assessments and privacy reviews are completed by the Attest Legal Team when new systems which process Respondent Personal Data are introduced.
Measures for allowing data portability and ensuring erasure	Attest allows customers to export their survey responses from the Attest platform during the course of a customer's subscription and encourages customers to download their survey data on an ongoing basis. Attest also has a process that is managed by the Attest Legal Team which allows data subjects to exercise their privacy rights, as set out in Attest's privacy policy.