Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the Master Services Agreement entered into between the Client and Pureprofile ("**Master Agreement**"), and governs Pureprofile's Processing of Personal Data.

AGREED TERMS:

1. Definitions and Interpretation

1.1. Unless otherwise defined in this DPA, capitalized terms and expressions used in this DPA shall have the meanings set out below:

"**Agreed Purposes**" means the provision, and enjoyment of the benefit, of the Services pursuant to the Master Agreement;

"**Client**" means the entity which has entered into a Master Agreement with Pureprofile;

"**Client Personal Data**" means any Personal Data Processed by Pureprofile on behalf of the Client pursuant to or in connection with the Master Agreement;

"**Data Discloser**" means a Party that discloses Personal Data to the other Party pursuant to the Master Agreement;

"**Data Protection Laws**" means all applicable data protection and privacy legislation in force from time to time which are applicable to either Party or to the services to be provided pursuant to the Master Agreement, which may include (but shall not be limited to) the EU GDPR, the UK GDPR, and the UK Data Protection Act 2018;

"**DPA**" means this Data Processing Agreement and all of its Schedules;

"**EEA**" means the European Economic Area;

"**EU GDPR**" means EU General Data Protection Regulation ((EU) 2016/679);

"**ICO**" means the UK Information Commissioner's Office;

"**Party**" means a party to this DPA, being either the Client or Pureprofile (and "Parties" shall be interpreted accordingly);

"**SCCs**" means the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the EU GDPR as set out in the Annex to Commission Implementing Decision (EU) 2021/914;

"**Services**" means the all-in-one, self-service platform for survey creation, online sampling, automated analytics, support services and other services, and cloud-based platform infrastructure that Pureprofile provides to the Client pursuant to the Master Agreement.

"**Subprocessor**" means any person appointed by or on behalf of Pureprofile to process Client Personal Data in connection with the Master Agreement.

"**UK**" means the United Kingdom of Great Britain and Northern Ireland.

"**UK GDPR**" has the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2. The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as given in the EU GDPR, and their cognate terms shall be construed accordingly.

1.3. This DPA forms part of, and is incorporated into, the Master Agreement.

1.4. Any reference to this DPA includes its Schedules.

1.5. A reference to writing or written includes email.

1.6. In the case of conflict or ambiguity between:

1. any provision contained in the body of this DPA and any provision contained in a Schedule, the provision in the Schedule will prevail; or

2. any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail.

2. Pureprofile as Controller

2.1. This clause 2 applies where Pureprofile acts as a Controller in relation to Personal Data shared with the Client pursuant to the Master Agreement.

2.2. Each Party shall comply with the obligations imposed on a Controller under the Data Protection Laws.

2.3. Each Party shall:

1. ensure that it has all necessary notices and consents and lawful bases in place to enable the lawful transfer of Personal Data to the other Party for the Agreed Purposes;

2. process the Shared Personal Data only for the Agreed Purposes;

3. not disclose or allow access to the Shared Personal Data to any third Party, unless otherwise agreed with the Data Discloser; and

4. ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the other Party, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

2.4. Each Party shall assist the other in complying with all applicable requirements of the Data Protection Laws. In particular, each Party shall:

1. assist the other Party, at the cost of the other Party, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, Personal Data Breach notifications, data protection impact assessments and consultations with the ICO, a Supervisory Authority or other regulators;

2. notify the other Party without undue delay on becoming aware of any breach of the Data Protection Laws; and

3. maintain complete and accurate records and information to demonstrate its compliance with this clause 2.

3. Pureprofile as Processor

3.1. This clause 3 applies where Pureprofile acts as a Processor on behalf of the Client in relation to Client Personal Data.

3.2. The table below describes the subject matter, duration, nature and purpose of the Processing and the Personal Data categories and Data Subject types in respect of which Pureprofile may Process the Client Personal Data for the purposes of providing the Services to the Client pursuant to the Master Agreement.

Subject matter, nature and purpose of Processing	Pureprofile shall Process the Client Personal Data for the purpose of providing the Services under the Master

	Agreement.
Duration of Processing	The duration of the Master Agreement.
Categories of Personal Data	The types of Personal Data described in the Master Agreement or otherwise agreed in writing between the parties from time to time, but which will typically include (without limitation) the Data Subject's name, telephone number(s), email address and home address.
Categories of Data Subjects	Participants in surveys carried out on the Client's behalf using Pureprofile's online platform.

3.3. Pureprofile shall comply with all applicable Data Protection Laws in the Processing of Client Personal Data.

3.4. Pureprofile shall not Process Client Personal Data other than on the Client's documented instructions. The Client instructs Pureprofile to process Client Personal Data as required in order to provide the Services pursuant to the Master Agreement. Pureprofile will not process the Client Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Laws. Pureprofile must promptly notify the Client if, in its opinion, the Client's instructions do not comply with Data Protection Laws.

3.5. Pureprofile will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Client or this DPA specifically authorises the disclosure, or as required by domestic law, court or regulator.

3.6. Pureprofile will reasonably assist the Client, at the Client's expense, with meeting the Client's compliance obligations under the Data Protection Laws, taking into account the nature of Pureprofile's processing and the information available to Pureprofile, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with any relevant regulator under the Data Protection Laws.

3.7. Pureprofile shall:

1. promptly notify the Client if it receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data; and

2. ensure that it does not respond to that request except on the documented instructions of Client or as required by applicable laws to which the Pureprofile is subject, in which case Pureprofile shall to the extent permitted by applicable laws inform the Client of that legal requirement before Pureprofile responds to the request.

3.8. Pureprofile shall provide reasonable assistance to the Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required by article 35 or 36 of the EU GDPR or the UK GDPR, as the context requires or equivalent provisions of any other Data Protection Laws, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, the Subprocessors.

3.9. Pureprofile will ensure that all of its employees and other personnel:

1. are informed of the confidential nature of the Client Personal Data and are bound by

confidentiality obligations and use restrictions in respect of the Client Personal Data;

2. have undertaken training on the Data Protection Laws relating to handling Personal Data and how it applies to their particular duties; and

3. are aware both of Pureprofile's duties and their personal duties and obligations under the Data Protection Laws and this DPA.

3.10. Taking into account 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, Pureprofile shall in relation to the Client Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the EU GDPR or the UK GDPR, as the context requires. In assessing the appropriate level of security, Pureprofile shall take account in particular of the risks that are presented by the proposed Processing, in particular from a Personal Data Breach.

3.11. Pureprofile shall notify Client without undue delay upon Pureprofile becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow the Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. Pureprofile shall co-operate with the Client and take reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

3.12. Subject to clause 3.13, on termination of the Master Agreement for any reason, or the expiry of its term, Pureprofile shall securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any of the Personal Data related to this DPA or the Master Agreement in its possession or control.

3.13. If any law, regulation, or government or regulatory body requires Pureprofile to retain any documents or materials or Client Personal Data that Pureprofile would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents, materials or Client Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

3.14. Pureprofile will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data. Pureprofile shall provide the Client with copies of such documentation as the Client may reasonably request in order to audit Pureprofile's compliance with this DPA.

3.15. Pureprofile engages various third parties to Process Personal Data in order to provide the Services ("**Subprocessors**"). Those Subprocessors approved as at the commencement of this DPA are as follows:

1. SightX Inc (provider of a survey research platform which may be used by Pureprofile to deliver the Services); and

2. Amazon Web Services (AWS), which provides cloud storage services;

3. Google (Google Cloud Workspace) which Pureprofile may use for cloud storage and backup services; and

4. Alchemer, Confirmit and Decipher which provide survey software tools which may be used by Pureprofile in order to deliver the Services.

3.16. Pureprofile may only authorise a new Subprocessor to process the Personal Data if the Client is provided with an opportunity to object to the appointment of such Subprocessor within 30 days after Pureprofile supplies the Client with details of the new Subprocessor.

3.17. Pureprofile will enter into a written contract with each Subprocessor that contains terms substantially the same as those set out in this clause 3, in particular, in relation to requiring appropriate technical and organisational data security measures to protect Client Personal Data.

3.18. Where a Subprocessor fails to fulfil its data protection obligations under its agreement with Pureprofile, Pureprofile will remain fully liable to the Client for the Subprocessor's acts and omissions to the same extent that Pureprofile would be liable if performing the relevant services directly under this DPA.

4. Transfers of Client Personal Data

4.1. Pureprofile (and any Subprocessor) may only transfer Client Personal Data from the UK or the EEA if:

1. the transfer of the Client Personal Data is to a territory which is subject to adequacy regulations under the Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals; or

2. Pureprofile participates in a valid cross-border transfer mechanism under the Data Protection Laws, so that Pureprofile (and, where appropriate, the Client) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and EU GDPR (as relevant).

4.2. If the transfer of any Personal Data from Pureprofile to the Client requires execution of standard data protection clauses adopted by the European Commission or another Supervisory Authority in accordance with Article 46 of the EU GDPR or UK GDPR (as appropriate), the relevant data protection clauses as completed and set out in the Schedule identified in the table below shall apply to such transfer of Personal Data.

Nature of transfer	**Applicable Data Protection Laws**	**Data protection clauses**	**As set out in:**
Pureprofile (acting as a Controller) transfers Personal Data to Client (acting as a Controller)	EU GDPR	SCCs – Module 1 (Controller to Controller)	Schedule 1
Pureprofile (acting as a Processor) transfers Personal Data to Client (acting as a Controller)	EU GPDR	SCCs – Module 4 (Processor to Controller)	Schedule 2
Pureprofile (acting as a Controller) transfers Personal Data to Client (acting as a Controller)	UK GDPR	UK International Data Transfer Addendum to the SCCs	Schedule 3
Pureprofile (acting as a Processor) transfers Personal Data to Client (acting as a Controller)	UK GDPR	UK International Data Transfer Addendum to the SCCs	Schedule 4

5. Term and Termination

5.1. This DPA will remain in full force and effect so long as:

1. the Master Agreement remains in effect; or

2. Pureprofile retains any of the Personal Data related to the Master Agreement in its possession or control.

5.2. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

6. **Notices**.

Any notice given to a Party under or in connection with this DPA shall be in writing and shall be given in accordance with the terms of the Master Agreement.

7. Governing Law and Jurisdiction

7.1. This DPA is governed by the laws of New South Wales, Australia.

7.2. Any dispute arising in connection with this DPA, which the Parties are not able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of New South Wales, Australia, subject to possible appeal to New South Wales, Australia.

SCHEDULE 1

Standard Contractual Clauses - Controller-to-Controller Transfers

SECTION I

CLAUSE 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each data importer)

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

CLAUSE 9 - Use of sub-processors

N/A

CLAUSE 10 - Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

CLAUSE 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

CLAUSE 13 - Supervision

(a) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Republic of Ireland.

CLAUSE 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of The Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data Exporter	
Name	Pureprofile Australia Pty Ltd
Address	263 Riley St, Surry Hills NSW, Australia 2010
Contact person's name, position and contact details	Niamh Fitzpatrick, Chief Product and Technology Officer niamh.fitzpatrick@pureprofile.com
Activities relevant to the data transferred under these Clauses	Providing the Client with access to Pureprofile's all-in-one, self-service platform for survey creation, online sampling, automated analytics, support services and other services, and cloud-based platform infrastructure. Pureprofile's platform will process personal data generated by the Client through surveys performed using the platform.
Role	Controller
Signature and date	Pureprofile will be deemed to have signed this Annex I on the transfer of Personal Data by Pureprofile to the Client in connection with the Services.

Data Importer	
Name	The Client
Address	The Client's address as set out in the Master Agreement
Contact person's name, position and contact details	The name, position and contact details provided by the Client to Pureprofile.
Activities relevant to the data transferred under these Clauses	Processing Personal Data received from Pureprofile in order to receive the benefit of the Services pursuant to the Master Agreement.
Role	Controller

Signature and date	By using the Services to transfer Personal Data to Pureprofile, the Client will be deemed to have signed this Annex I.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Individuals who participate in surveys through Pureprofile's online platform.
Categories of personal data transferred	As described in the Master Agreement.
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.	As described in the Master Agreement.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Data may be transferred on a one-off or continuous basis for the purposes of providing the Client with the Services pursuant to the Master Agreement.
Nature of the processing	The Personal Data will be Processed and transferred for the purpose of providing the Client with the Services pursuant to the Master Agreement.
Purpose(s) of the data transfer and further processing	The Personal Data will be Processed and transferred for the purpose of providing the Client with the Services pursuant to the Master Agreement, including market research and providing customer support.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Such period as may be agreed with the Client in the Master Agreement, or otherwise determined by Pureprofile on a case-by-case basis.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	**1.** SightX Inc provides a survey research platform which may be used by Pureprofile to deliver the Services. **2.** Pureprofile may transfer Personal Data to Amazon Web Services (AWS), which provides cloud storage services.

	3. Pureprofile may transfer Personal Data to Google (Google Cloud Workspace) which Pureprofile may use for cloud storage and backup services. **4.** Pureprofile may transfer Personal Data to Alchemer, Confirmit and Decipher, which provide survey software tools which may be used by Pureprofile in order to deliver the Services. In each case, the Personal Data would be processed for such period as is necessary to enable Pureprofile to deliver the Services.

C. COMPETENT SUPERVISORY AUTHORITY

The BfDI – The Federal Commissioner for Data Protection and Freedom of Information in Germany

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Encryption of all data at REST using AES-256 specification;

- Encryption of all data in Transit using TLS v.1.2 with AES-256 encryption cipher;
- Access to systems only via whitelisted and/or Pureprofile’s VPN IPs and using individual private keys;
- Separation of development, testing and production environments;
- Databases are not connected to the public internet but only accessible by applications within the respective VPCs;
- Internal penetration testing performed once a quarter or after major code changes;
- Penetration testing performed by independent 3rd Party once a year
- ISO 20252:2019
- ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems

-

Schedule 2

Standard Contractual Clauses - Processor-to-Controller Transfers

SECTION I

CLAUSE 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4 - Interpretation

(c) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(d) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(e) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

CLAUSE 9 - Use of sub-processors

N/A

CLAUSE 10 - Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

CLAUSE 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

CLAUSE 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

CLAUSE 13 - Supervision

N/A

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14 - Local laws and practices affecting compliance with the Clauses (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15 - Obligations of the data importer in case of access by public authorities *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(c) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(d) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(e) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 17 - Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Republic of Ireland.

CLAUSE 18 - Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of The Republic of Ireland.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data Exporter	
Name	Pureprofile Australia Pty Ltd
Address	263 Riley St, Surry Hills NSW, Australia 2010
Contact person's name, position and contact details	Niamh Fitzpatrick, Chief Product and Technology Officer niamh.fitzpatrick@pureprofile.com
Activities relevant to the data transferred under these Clauses	Providing the Client with access to Pureprofile's all-in-one, self-service platform for survey creation, online sampling, automated analytics, support services and other services, and cloud-based platform infrastructure. Pureprofile's platform will process personal data generated by the Client through surveys performed using the platform.
Role	Processor
Signature and date	Pureprofile will be deemed to have signed this Annex I on the transfer of Personal Data by Pureprofile to the Client in connection with the Services.

Data Importer

Name	The Client
Address	The Client’s address as set out in the Master Agreement
Contact person’s name, position and contact details	The name, position and contact details provided by the Client to Pureprofile.
Activities relevant to the data transferred under these Clauses	Processing Personal Data received from Pureprofile in order to receive the benefit of the Services pursuant to the Master Agreement.
Role	Controller
Signature and date	By using the Services to transfer Personal Data to Pureprofile, the Client will be deemed to have signed this Annex I.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Individuals who participate in surveys through Pureprofile’s online platform.
Categories of personal data transferred	As described in the Master Agreement.
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.	As described in the Master Agreement.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Data may be transferred on a one-off or continuous basis for the purposes of providing the Client with the Services pursuant to the Master Agreement.
Nature of the processing	The Personal Data will be Processed and transferred for the purpose of providing the Client with the

	Services pursuant to the Master Agreement.
Purpose(s) of the data transfer and further processing	The Personal Data will be Processed and transferred for the purpose of providing the Client with the Services pursuant to the Master Agreement, including market research and providing customer support.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Such period as may be agreed with the Client in the Master Agreement, or otherwise determined by Pureprofile on a case-by-case basis.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	**1.** SightX Inc provides a survey research platform which may be used by Pureprofile to deliver the Services. **2.** Pureprofile may transfer Personal Data to Amazon Web Services (AWS), which provides cloud storage services. **3.** Pureprofile may transfer Personal Data to Google (Google Cloud Workspace) which Pureprofile may use for cloud storage and backup services. **4.** Pureprofile may transfer Personal Data to Alchemer, Confirmit and Decipher, which provide survey software tools which may be used by Pureprofile in order to deliver the Services. In each case, the Personal Data would be processed for such period as is necessary to enable Pureprofile to deliver the Services.

Schedule 3

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

PART 1: The Parties

Table 1: The Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name (and trading name, if different): Pureprofile Australia Pty Ltd	Full legal name (and trading name, if different): The Client
	Main address (if a company registered address): 263 Riley Street, Surry Hills NSW, Australia 2010	Main address (if a company registered address): The Client's address as set out in the Master Agreement
	Official registration number (if any) (company number or similar identifier): ABN 99 093 819 713	Official registration number (if any) (company number or similar identifier): The Client's registration number as set out in the Master Agreement
Key contacts	Niamh Fitzpatrick, Chief Product and Technology Officer niamh.fitzpatrick@pureprofile.com	The name, position and contact details provided by the Client to Pureprofile
Signature	By using the Services to transfer Personal Data to the Client, Pureprofile will be deemed to have signed this UK International Data Transfer Addendum.	The Client will be deemed to have signed this UK International Data Transfer Addendum on the transfer of Personal Data by Pureprofile in connection with the Services.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	**Module in operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**

1	Module 1	No	No	General Authorisation	30 days	No

Table 3: Appendix Information

This Table 3 (Appendix Information) is deemed to be populated with the information included in the Appendix to the SCCs (Module 1), as set out in Schedule 1 to this DPA and the Appendix to the SCCs (Module 4) as set out in Schedule 2 to this DPA, as relevant.

Table 4: Ending this Addendum when the Approved Addendum changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter

PART 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs, those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCS The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information As set out in Table 3.

Appropriate Safeguards The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) of the UK GDPR.

Approved Addendum The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

ICO The Information Commissioner.

Restricted Transfer A transfer which is covered by Chapter V of the UK GDPR.

UK The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

(a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

(b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

(c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

(b) In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

(c) Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

(d) Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

(f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(g) References to Regulation (EU) 2018/1725 are removed;

(h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "the UK";

(i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(l) In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    (a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    (b) reflects changes to UK Data Protection Laws.

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    (a) its direct costs of performing its obligations under the Addendum; and/or

    (b) its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Schedule 4

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES (Processor to Controller)

PART 1: The Parties

Table 1: The Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name (and trading name, if different): Pureprofile Australia Pty Ltd	Full legal name (and trading name, if different): The Client
	Main address (if a company registered address): 263 Riley Street, Surry Hills NSW, Australia 2010	Main address (if a company registered address): The Client's address as set out in the Master Agreement
	Official registration number (if any) (company number or similar identifier): ABN 99 093 819 713	Official registration number (if any) (company number or similar identifier): The Client's registration number as set out in the Master Agreement
Key contacts	Niamh Fitzpatrick, Chief Product and Technology Officer niamh.fitzpatrick@pureprofile.com	The name, position and contact details provided by the Client to Pureprofile
Signature	By using the Services to transfer Personal Data to the Client, Pureprofile will be deemed to have signed this UK International Data Transfer Addendum.	The Client will be deemed to have signed this UK International Data Transfer Addendum on the transfer of Personal Data by Pureprofile in connection with the Services.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	**Module in operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**
4	Module 4	No	No	General	30 days	No

				Authorisation		

Table 3: Appendix Information

This Table 3 (Appendix Information) is deemed to be populated with the information included in the Appendix to the SCCs (Module 1), as set out in Schedule 1 to this DPA and the Appendix to the SCCs (Module 4) as set out in Schedule 2 to this DPA, as relevant.

Table 4: Ending this Addendum when the Approved Addendum changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter

PART 2: Mandatory Clauses

Entering into this Addendum

21. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

22. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

23. Where this Addendum uses terms that are defined in the Approved EU SCCs, those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCS The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information As set out in Table 3.

Appropriate Safeguards The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) of the UK GDPR.

Approved Addendum The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

ICO The Information Commissioner.

Restricted Transfer A transfer which is covered by Chapter V of the UK GDPR.

UK The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR As defined in section 3 of the Data Protection Act 2018.

24. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

25. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

26. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

27. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

28. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

29. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

30. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

31. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

32. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

(a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

(b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

(c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

33. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

34. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

35. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

(b) In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

(c) Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

(d) Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

(f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(g) References to Regulation (EU) 2018/1725 are removed;

(h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "the UK";

(i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(l) In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

36. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

37. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

38. From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

39. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

40. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.