Toluna Data Share Terms

(A) Toluna and Client either entered into a Proposal, subject to Toluna standard Terms and Conditions ("**Terms**") or a SOW pursuant to a Master Services Agreement ("**MSA**") that covers the performance of the Services contemplated herein;

(B) Pursuant to sub-clause 15.4.2 of the Terms, the parties agreed under the Proposal that the Services may require the disclosure, by Toluna to the Client, or collection by the Client, of Shared Personal Data (defined below). In respect of such Shared Personal Data, the Client will also be an independent controller. Toluna wishes the Shared Personal Data to remain confidential and protected from unauthorised access by and /or use by the Client and/or disclosure to, third parties;

(C) The parties each acknowledge their responsibilities under applicable data protection law; and

(D) Client agrees to maintain, the security, integrity and confidentiality of the Shared Personal Data in accordance with the terms, covenants, obligations, representations, warranties and agreements contained in this Agreement.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. Definitions:

"**Affiliate**" means in relation to a party to this Agreement, any corporation or other entity that controls, is controlled by, or is under common control with, a party. A corporation or other entity shall be regarded as in control of another corporation or entity if it owns or directly or indirectly controls 50% or more of the voting securities or other ownership interest of the other corporation or entity, or if it possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the corporation or other entity.

"**Data Protection Legislation**" means all applicable local laws or regulations relating to the processing of personal data as contemplated under this Agreement, including in particular, but not limited to, the following as amended, extended or re-enacted from time to time: (i) EC Directive 2002/58/EC on Privacy and Electronic Communications; (ii) GDPR; (iii) the UK GDPR; (iv) USA Data Privacy Laws; and (v) LGDP; ; and

the terms "**personal data**", "**controller**", "**process**", "**processing**", "**processor**", "**data subject**", "**personal data breach**" and "**supervisory authorities**" shall have the meaning ascribed to them in the GDPR.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and any other directly applicable EU legislation relating to privacy and/or data protection.

"**Guidelines**" means generally accepted professional industry standards and practices for survey research including any guidelines or codes of conduct published by ESOMAR (The World Association of Research Professionals);

"**LGDP**" means the General Personal Data Protection Act Law No. 13.709 / 2018 (Lei Geral de Proteção de Dados Pessoais).

"**Proposal**" has the meaning given to it under the Terms.

"**Purpose**" for the purposes specified the Appendix.

"**Respondent**" means an individual who responds to a survey located in the countries specified in the Proposal.

"**Services**" means the services described in the Proposal.

"**Shared Personal Data**" means personal data about the Respondents, being those Personal Data listed in the Appendix and which the parties each control.

"Standard Contractual Clauses" or "SCC's" means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the GDPR in accordance with the EC Decision EU 2021/914 on 4 June 2021 (Module 1; Controller to Controller) (as may be amended or replaced by the European Commission from time to time) and attached hereto at Appendix A.

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

"**USA Data Privacy Laws**" means any US state law concerning the processing of personal data, as implemented in the relevant US state, including, but not limited to: **the California Consumer Privacy Act 2018, Cal. Civ. Code §§ 1798.100 et seq. (as amended by the CPRA)** ("**CCPA**"); Colorado Privacy Act 2021 (SB 190); Connecticut Data Privacy Act 2022 (SB 6); Delaware Personal Data Privacy Act 2023 (HB154); Iowa Consumer Data Protection Act 2023 (SF 262); Montana Consumer Data Privacy Act 2023 (SB 384); Nebraska Data Privacy Act 2024 (LB 1074); New Hampshire Data Privacy Law 2024 (SB 255); New Jersey Data Privacy Law 2024 (SB 332); Oregon Consumer Privacy Act 2023 (SB 619); Texas Data Privacy and Security Act (2023 (HB 4); Utah Consumer Privacy Act 2022 (SB 227); Virginia Consumer Data Protection Act 2021 (SB 1392); Indiana Consumer Data Protection Act 2023 (SB 5); Kentucky Consumer Data Protection Act 2024 (HB 15; Maryland Online Data Privacy Act 2024 (SB 541); Minnesota Consumer Data Privacy Act 2024 (HF 4757); Rhode Island Data Transparency and Privacy Protection Act 2024 (H 7787); and Tennessee Information Protection Act 2023 (HB 1181); **(when in force).**

"**SOW**" means a Statement of Work or work order under the terms of the MSA as agreed between the parties upon receipt of an order from the Client or acceptance of a service by the Client, which may set forth, amongst other things, the pricing, pricing terms and delivery and other terms relating to the performance of the services.

2. Representations and Warranties

2.1 Client hereby represents, warrants and undertakes that it will:

(a) use the Shared Personal Data solely for a Purpose, which shall be for exclusively research purposes, permitted under the Guidelines;

(b) not allow the Shared Personal Data to be transferred to any other party, except to its permitted processors who process the Shared Personal Data on its behalf for the Purpose;

(c) not use or allow any portion of the Services (including any personal data it processes about the Respondents) to match or link with any other data Client or third party may have or acquire, where such matching or linking will enable a Respondent to be identified or re-identified, in particular, Client shall ensure that the Respondents' identity cannot be inferred via deductive disclosure (for example, through cross-analysis, small samples or in combination with other data such as client's records or secondary data in the public domain);

(d) not allow any Respondents to be identified by its end clients (if any);

(e) erase all the Shared Personal Data immediately upon completion of the Purpose (and in any event within 30 days of the end of the research relevant to such processing);

(f) not recruit, or attempt to recruit any Respondent into any panel, community or group of individuals, online or off-line, or take any action that would allow the Client to contact, or allow any other party to contact any Respondent, or recruit him/her for any other market research activities, or any other activities at any time in the future;

(g) not process the Shared Personal Data for any use which is contrary to the Guidelines including, without limitation for marketing, promotional, selling or influencing the opinions or decisions of any Respondent;

(h) collect the Shared Personal Data fairly and lawfully and in accordance with this Agreement and the Data Protection Legislation;

(i) ensure that the Respondents are not Minors, unless the Respondents' parents or guardians have provided their unambiguous consent to process their personal data for the Purpose;

(j) maintain complete and accurate records and information to demonstrate its compliance with this Clause 2 and allow for audits by Toluna or Toluna's designated auditor;

(k) (if relevant) complete and sign the SCC's;

(l) put appropriate technical and operational processes and procedures in place to safeguard against unauthorised or unlawful processing of the Shared Personal Data; (ii) protect the security, integrity and confidentiality of the Shared Personal Data and will not permit any unauthorised access to, or use, disclosure, publication or dissemination of, the Shared Personal Data and against accidental loss or destruction of, or damage to, Shared Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Shared Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Shared Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it). Client agrees to use the same degree of care and scrutiny as it uses to protect and secure its own confidential information and customer information, but in no event will Client use less than a reasonable degree of care; and

(m) in the event of a breach of the security of Client's systems, servers and/or facilities, or any unauthorised access to, or use and/or disclosure of the Shared Personal Data ("**Security Breach**"), whilst in Client's possession Client will promptly notify Toluna, but in no event later than twenty-four (24) hours, after Client first learns of or discovers the Security Breach. In the event of a Security Breach, Client will (i) use its best efforts to mitigate any harmful effect(s) of the Security Breach; (ii) use commercially reasonable efforts to make available sufficient resources and data for Toluna to determine the full impact and root cause of the Security Breach; and (iii) fully co-operate with Toluna in investigating the cause(s) of any Security Breach and in providing notice to affected individuals and/or the appropriate legal and/or regulatory agencies, as required by any Data Protection Legislation or applicable laws and codes of practice.

2.2 Client shall indemnify, defend and hold harmless Toluna and its affiliates, officers, directors, agents, successors and assigns from and against any third party claims and related losses, damages, fines, penalties and expenses, including reasonable attorney's' fees, that arise out of or result from Client's breach of this clause 2.

3. Compliance with laws, including the Data Protection Legislation

3.1 **General.** It is acknowledged and agreed that the parties are independent controllers under the Data Protection Legislation. As such, both parties shall, in a transparent manner determine their respective responsibilities for compliance with the obligations under the Data Protection Legislation.

3.2 **Privacy notices.** Each party shall ensure that its' privacy notices to Respondents are prominently displayed, clear and provide sufficient information to them to understand what of their personal data will be shared with whom, the circumstances in which they will be shared, the purposes for which their personal data will be shared and either the identity of such recipients or a description of the type of organisation that will receive the Shared Personal Data.

3.3 **Processing of Personal Data.** Each party shall: (a) comply with all Data Protection Legislation in the processing of Shared Personal Data; and (b) not process Shared Personal Data except as necessary to perform the Services, unless such processing is required by Data Protection Legislation. The parties shall take steps necessary to ensure the reliability of any employee, agent or contractor who may have access to Shared Personal Data, ensuring that access is limited to those individuals who

need to know or access Shared Personal Data as strictly necessary to perform the Services and ensuring that all such individuals comply with Data Protection Legislation.

3.4 **Data processors.** When appointing data processors, all parties shall: (i) carry out adequate due diligence before the Data processor processes the Shared Personal Data to ensure the Data processor is capable of complying with the terms for data processors under Article 28 GDPR; and (ii) enter into a written agreement with each data processor on terms required under Article 28 GDPR.

3.5 **Data Subject Rights.** If Client receives a request from a data subject under Data Protection Legislation in respect of Shared Personal Data, the Client should notify Toluna of such request within forty-eight (48) hours of receipt of such request to enable Toluna to respond to such request as required under Data Protection Legislation. Client will assist Toluna, at Client's cost, in responding to any request from a data subject and in ensure compliance with its obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

3.6 **Personal data breach.** In the event of a personal data breach, all parties shall comply with all obligations under Data Protection Legislation in respect to the mitigation, and remediation of any personal data breach. Where a personal data breach involves the Shared Personal Data, such mitigation and remediation may include, without limitation, the provision of notice to any affected or potentially affected data subjects, and supervisory authorities. All parties and its data processors shall take any and all measures necessary to minimize the adverse impacts of the personal data breach, to restore the security, confidentiality, and/or integrity of the Shared Personal Data, and to prevent a recurrence of any personal data breach.

3.7 **Retention of personal data.** Each party should have in place a data retention policy specifying the length of time it will keep personal data for and should securely erase the Shared Personal Data that are no longer needed for the purpose for which they were obtained.

3.8 **Restricted Transfers.** Transfers of the Shared Personal Data outside the country in which the Respondents reside may be a restricted transfer under the Data Protection Legislation and may require the written authorisation of the Respondents and/or entering into data transfer agreements (e.g. the SCC's) as required under the Data Protection Legislation and the parties hereby confirm they have entered into the SCC's, where applicable and shall enter into any other such data transfer agreements as may be required by law.

3.9 **Audit Rights**. The parties shall make available to the other party upon reasonable request or as required by Data Protection Legislation all information necessary to demonstrate compliance with the Agreement.

3.10 **Indemnity.** Each party shall indemnify, defend and hold harmless the other party and their respective affiliates, officers, directors, agents, successors and assigns from and against any third party claims and related losses, damages, fines, penalties and expenses, including reasonable attorney's' fees, that arise out of or result from either party's breach of this clause 3 capped to one million pounds (£1,000,000).

THE APPENDIX

Categories of Personal Data	**The Purposes**
Name and Contact data	Adverse Event reporting.
Name and Contact data	To allow Respondents to contact the Client for troubleshooting purposes.
IP address, Device ID and other technical identifiers as are strictly necessary for the Purpose	(i) Quality and fraud checking and (ii) troubleshooting purposes
Image and audio of the Respondent	To view and/or receive an online recording of a qualitative interview, subject to clause 2.1(e) above

APPENDIX A

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

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) (i) 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.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 anonymisation [ii] 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 [iii] (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. (iv) 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) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, 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 (v);

(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 FRANCE.

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 PARIS.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: **Toluna SAS**

Address: 5, Avenue du Château, 94300 Vincennes, France

Contact person's name, position and contact details:

ANNE-MARIE HORGAN – GROUP DPO

DPO@TOLUNA.COM

Activities relevant to the data transferred under these Clauses:

Data exporter is a global market research panel company and has agreed that the data importer may process personal data about its panel members for market research purposes under the Toluna Data Share Terms and Proposal or SOW ("**DSA**").

Signature and date: 

Role (controller): General Counsel

Data importer(s):

Name: The Client specified in the DSA

Address: The Client address as specified in the DSA

Contact person's name, position and contact details: The Client contacts as specified in the DSA

Activities relevant to the data transferred under these Clauses: As specified in the DSA

Signature and date: Signed and/or agreed to by the Client in the DSA

Role (controller):

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The Respondents specified in the DSA

Categories of personal data transferred

For the purposes specified in the DSA

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.*

N/A

The frequency of the transfer *(e.g. whether the data is transferred on a one-off or continuous basis).*

One off basis

Nature of the processing

As agreed in the DSA

Purpose(s) of the data transfer and further processing

For market research purposes and specifically for the Purpose as set out in the DSA.

The period for which the personal data will be retained*, or, if that is not possible, the criteria used to determine that period*

Data importer shall erase the personal data in accordance with clause 2.1(e) of the DSA.

C. COMPETENT SUPERVISORY AUTHORITY

Commission nationale de l'informatique et des libertés (**CNIL**)

ANNEX II

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

Data importer undertakes technical and organisational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons, including measures addressing the following:

- pseudonymisation and encryption of personal data.
- ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.
- user identification and authorisation.
- the protection of data during transmission, such as SFTP use and encryption in transit.
- protection of data during storage.
- ensuring physical security of locations at which personal data are processed.
- ensuring events logging.
- ensuring system configuration, including default configuration.
- internal IT and IT security governance and management.
- certification/assurance of processes and products
- ensuring data minimising.
- ensuring data quality.
- ensuring limited data retention.
- ensuring accountability.
- allowing data portability and ensuring erasure.