IPSOS PURCHASING TERMS
Valid for Ipsos GmbH and trend.test Gesellschaft für telefonische Datenerhebung mbH
(both hereinafter referred to as „Ipsos")

Version 18. November 2026

0**. Contractual Documents. If** a separate agreement is signed between the parties related to the Services covered hereunder, then such agreement shall take precedence over the Ipsos Purchasing Terms set forth herein. Where no separate agreement exists, each purchase order ("**Purchase Order**") placed by Ipsos for goods and/or services/or deliverables covered hereunder (the "**Services**") is subject to these Ipsos Purchasing Terms ("**Ipsos Purchasing Terms**", or "**Terms**", or the "**Agreement**" as referred to herein) and the terms of the applicable Purchase Order. No other document, including Vendor's terms or conditions or any proposals, shall prevail over the Ipsos Purchasing Terms. Vendor shall be deemed to have agreed to be bound by such Ipsos Purchasing Terms by accepting the Purchase Order and/or commencing the performance of the Services.

Where either (i) Services may be performed by Vendor in the absence of a Purchase Order, or (ii) a Purchase Order agreed by the parties may not be fully executed, the parties agree that should either of the two foregoing circumstances occur, Ipsos Purchasing Terms shall nevertheless govern the rights and obligations of the parties with respect to the Services provided by Vendor.

The Agreement consists only of: (a) these Ipsos Purchasing Terms; (b) the applicable Purchase Order; and (c) any specifications or other documents expressly referenced in the Purchase Order. Any reference in the Purchase Order to any Vendor's proposal is solely for the purpose of incorporating the descriptions and specifications of the Services contained in the proposal, and only to the extent that the terms of the Vendor's proposal do not conflict with the Terms and the descriptions and specifications set out in the Purchase Order. Ipsos' acceptance of, or payment for, the Services will not constitute Ipsos' acceptance of any additional or different terms in any Vendor proposal, unless otherwise accepted in writing by Ipsos. If there is any conflict or inconsistency between the documents constituting the Agreement, then unless otherwise expressly provided, the documents will rank in the order of precedence in accordance with the order in which they are listed in this clause.

Notwithstanding anything to the contrary in the Ipsos Purchasing Terms, Ipsos shall have no obligation to purchase the Services exclusively from Vendor, and Ipsos may use other service providers of its choice for any and all services and/or deliverables identical or similar to the Services and/or Deliverables provided by Vendor under the Agreement and the relevant Purchase Order. Nothing in this Agreement shall be construed to constitute any guarantee or commitment from Ipsos to order any particular amount or volume of Services other than as explicitly set forth in a Purchase Order.

"Ipsos Affiliates" means with respect to Ipsos: any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, whether incorporated or not, that the French holding company Ipsos SA , or any of its subsidiaries , directly or indirectly holds 30% or more of the nominal value of the issued share capital or 30% or more of the voting power at General Meeting, and/or either (i) has the power to appoint a majority of directors, or (ii) when by contract or otherwise, can direct or cause the direction, or the management or the activities of such entity/Affiliate from time to time even if Ipsos SA or any of its subsidiaries has a minority interest in that entity.

1. **The Work and Acceptance of the Services.** Ipsos hereby engages Vendor to perform the Services as set forth in the Purchase Order (or any similar document) and incorporated herein. Vendor shall perform the Services pursuant to the specifications set forth in each Purchase Order, in a timely, diligent, and workmanlike manner, and with the highest professional standards of vendors who perform comparable services within or for the market research industry. Vendor will comply with (i) all relevant policies and codes of conduct of Ipsos as attached in **Annex 1** and (ii) the Ipsos end client policies. Time is of the essence in the performance of the Services. Ipsos will evaluate and either **"Accept"** or **"Reject"** the Services in accordance with the specifications listed in the applicable Purchase Order, within thirty (30) days of performance or delivery of such Services to Ipsos. Where Ipsos determines to reject the Services, Ipsos shall provide written notice to Vendor, which shall state the reason by referring to the applicable specification from the Purchase Order to which the Services do not conform. If the Services do not pass inspection because they do not conform to the specifications in the applicable Purchase Order, Vendor shall have the opportunity to cure and re-deliver the non-conforming Services, and the evaluation will be repeated until the new Services are accepted by Ipsos or Ipsos elects to terminate the Purchase Order. If Ipsos elects to terminate the Purchase Order, then Vendor will reimburse Ipsos the related fees that Ipsos may have paid in advance without prejudice to any damages Ipsos may ask. Acceptance will occur when the Services have been Accepted in accordance with the provisions of this Section. Any payment of fees by Ipsos to the Vendor does not, under any circumstances, imply Ipsos' acceptance of the Services or any Work Product to be provided by the Vendor under a Purchase Order.

   Vendor warrants to Ipsos that the Services shall comply with the specifications as listed in the relevant Purchase Order for ninety (90) business days after the Acceptance date and shall modify, repair or replace any Service which does not conform with the specifications or any documentation at no additional cost to Ipsos or as an alternative (at Ipsos choice) refund or credit Ipsos the Fees paid for such Services. If Ipsos does not accept or reject a Service within thirty (30) days following receipt of a Service, then Ipsos shall be deemed to have accepted these Services.

2. **Payment.** The fees for the Services shall be as set forth in the Purchase Order. Unless otherwise stated in a Purchase Order, all prices or other payments stated in the Purchase Order are exclusive of any taxes. If not agreed otherwise in the Purchase Order, Vendor will invoice Ipsos for the Services as follows: In the case of tracking studies requiring the periodic delivery of data, Vendor will invoice a pro-rated amount of the entire study costs on a monthly or quarterly basis as mutually agreed in the Work Order. In case of no tracking study and unless the billing schedule is set forth in the Work Order, all amounts due under the Work Order will be invoiced upon completion of the project. Ipsos will pay those invoices within sixty (60) days after the completion and Acceptance by Ipsos of the Services and Ipsos receives an invoice that is satisfactory to Ipsos in form and content. Effective January 1, 2027, the supplier is required to submit invoices exclusively in an electronic format that complies with the applicable legal requirements. In particular, the invoice must comply with the requirements of Section 14 of the German Value-Added Tax Act (UStG). In addition, it must comply with and be interoperable with the European standard EN 16931. Invoices that do not meet the legal requirements are considered improperly submitted. Ipsos is entitled to reject such invoices. Payment periods do not begin until a valid invoice is received. All costs associated with the preparation, transmission, and compliance with legal

requirements for electronic invoicing shall be borne by the supplier. Any out-of-pocket expenses incurred as a part of the Services rendered in a Purchase Order must be pre-approved by Ipsos in writing and shall include supporting documents with no mark-up. The invoice(s) for these expenses are to be submitted no more than 30 days after the Service has been rendered and paid in accordance with the terms and conditions of these Terms. Upon notice to Vendor, Ipsos may withhold payment(s) for any item(s) on Vendor's invoice(s) that Ipsos reasonably disputes. Pending settlement or resolution of the dispute, Ipsos' non-payment of such disputed items shall not per se constitute default by Ipsos and shall not entitle Vendor to suspend, delay or cease its furnishing of the Work product or performance of the Services. All the fees listed in a Purchase Order shall remain unchanged during the Term unless it is changed by Ipsos through a change of the Purchase Order.

In any case, the fees should not increase more than three (3%) for any renewal term.

3. **Term and Termination.** These Terms will commence and end on the dates set forth in the Purchase Order (the "**Term**"), unless earlier terminated as set forth herein. Either party shall have the right to terminate this Agreement, effective immediately, at any time and without prior notice, if the other party fails to cure a breach of this Agreement within thirty (30) days of receiving written notice of such breach by the non-breaching party. Either party may terminate this Agreement if (i) the other party has a receiver appointed for it or its property; (ii) the other party makes an assignment for the benefit of creditors; (iii) any proceedings are commenced by, for or against the other party under any bankruptcy, insolvency or debtor's relief law; (iv) the other party is liquidated or dissolved.

   In addition, Ipsos shall have the right to terminate this Agreement and/or any Purchase Order without cause upon thirty (30) days prior written notice to Vendor. Ipsos may terminate immediately this Agreement in case of Vendor's change of ownership involving an Ipsos' competitive entity.

   Notwithstanding anything herein to the contrary, if this Agreement is terminated by Ipsos for reasons that can be attributed to Vendor, Vendor shall refund to Ipsos any prepaid fees for Services that have not actually been delivered as of the effective date of the termination, and Ipsos shall not be liable for any future payments for such terminated Services from thereon.

   Termination or non-renewal of a Purchase Order shall not terminate any other Purchase Orders that are in place at the time of such termination or expiration, which shall continue until their completion under these Terms, unless Ipsos notifies in writing to Vendor a termination of a Purchase Order or all Purchase Orders or Services within three (3) business days before the termination date of the relevant Purchase Order.

   Upon termination of this Agreement for any reason, Vendor commits to (i) return to Ipsos any document or materials provided by Ipsos within a maximum period of ten (10) days of termination of this Agreement, and (ii) deliver to Ipsos the Work Product regardless of its completion status. Sections 4 to 11, and Sections 16, 17, 21 and 22 shall survive the termination of this Agreement. The termination and cancellation provisions set out in this Section are not exclusive, and are in addition to, and not in limitation of either party's rights under these Terms or at law and are without prejudice of any damages or service credits that Ipsos may claim.

4. Representations and Warranties.

4.1. General Representations and Warranties: Vendor represents and warrants that where the service performed pursuant to this Agreement constitute market, opinion or social research or data analytics, they shall be rendered in accordance with ISO 20252 as well as all generally accepted professional industry standards and practices applicable to the advertising and marketing research industry, including, without limitation, the International Code of Marketing and Social Research Practice issued by the ICC, ESOMAR and, if required by Ipsos, ADM standards. In addition, the Vendor represents and warrants that (i) it will comply with all applicable laws, rules and regulations, including applicable privacy and data protection laws as well as the German Mindestlohngesetz / Minimum Wage Act (if applicable) and applicable laws relating to corruption and/or bribery and U.S or non U.S. export control laws and regulations; (ii) it has obtained any and all permits, licenses and third party consents or approvals necessary in connection with the performance of its Services; (iii) the Services will conform in all material respects to the specifications in the Purchase Order and to any requirements and documentation; (iv) it shall commit to dedicate the necessary human resources to assist Ipsos with the provision and the implementation of the Services and to take all reasonable steps to maintain continuity in relation to its staff dedicated to the performance of the Services; (v) it shall both on its own behalf and on behalf of its personnel and its subcontractors, if any, comply with the procedures, technical procedures and policies in effect at Ipsos premises or sites where the Services will be performed; (vi) it will be solely responsible for the payment of its sub-processors and subcontractors and fully liable for the acts and/or omissions of any and all its sub-processors and subcontractors in the whole supply-chain as if they were Vendor hereunder; (vii) it is and shall remain at all times, owner of its tools, software, or equipment and every component thereof as well as owner of the related intellectual property rights and source codes, or the recipient of a valid license thereto; (viii) it has and will maintain the full power, and authority to grant the intellectual property rights and other rights granted in this Agreement without the further consent of any third party and that there is no restriction or limitation for the Vendor to transfer those intellectual property rights on the Services or the Work Product to Ipsos according to the terms of this Agreement or the relevant Purchase Order; (ix) the Services shall not violate or infringe upon the trademark, copyright, patent or other intellectual property rights or right of privacy or publicity of any third party; (x) the tools, software, or equipment and any media used to provide the Services contain no viruses or other destructive programming or computer instructions or technological means intended to disrupt, damage, or interfere with Ipsos' infrastructure as far as this is in Vendor's reasonable technical sphere of control; (xi) no third party software (including free or open-source software) will be included in the Services and in any Work Product without the written consent of Ipsos and Ipsos shall have no obligation to pay any third party any fees, royalties, or other payments for Ipsos' use of any third party software, (xii) it shall not use the name, logos or trademarks of Ipsos or any of Ipsos' end clients in any advertising, marketing or promotional materials, press releases or press conferences without Ipsos' prior written consent and (xiii) it shall procure that any of its subcontractors in the whole supply-chain shall at all times comply with the terms of this Agreement.

4.2. Sanctions Laws Representations and Warranties.

Definitions. For the purposes of this Section:

(a) "**Sanctions"** means any laws or regulations relating to economic or financial sanctions, export controls, trade embargoes or restrictive measures from time to time

imposed, issued, administered or enforced by any Sanctions Authority;

(b) **"Sanctions Authority"** means any governmental, judicial or regulatory institutions, agencies, departments and authorities of: (i) the US; (ii) the United Nations; (iii) the European Union ("EU") and European Economic Area ("EEA") and any EU or EEA Member State; (iv) Switzerland; and (v) the UK; and any other (i) authority or (ii) local, state, multi-state, national or multi-national government, under whose jurisdiction Ipsos and/or its activities fall, or which asserts jurisdiction over Ipsos and/or its activities (excluding any authorities of nations unfriendly to the US, EU, Switzerland and/or UK including, without limitation, Russia and Belarus);

(c) **"Sanctions List"** means any of the lists issued or maintained by a Sanctions Authority designating or identifying individuals or entities that are subject to Sanctions, in each case as amended, supplemented or substituted from time to time; and

(d) **"Sanctioned Person"** means an individual or entity on a Sanctions List, or an entity which is majority owned or controlled by that individual or entity.

4.2.1. The Vendor warrants and represents that the Vendor, each of the Vendor's shareholders, directors, officers, employees, agents or other associated persons, are not, and have not been, (i) a Sanctioned Person; (ii) in breach of Sanctions; or (iii) dealing with, or acting for the benefit of, a Sanctioned Person.

4.2.2. The Vendor shall not engage in any transactions or activities that would cause Ipsos to violate any Sanctions. This includes, but is not limited to, providing any software, platforms, technology, or any other technical support to any Russian or Belarusian entities or personnel to whom it subcontracts any portion of the Services.

4.2.3. The Vendor warrants and represents that the Vendor has implemented adequate policies and procedures to ensure its compliance with Sanctions and will maintain such policies and procedures up to date.

4.2.4. The Vendor will keep detailed, accurate and up-to-date records of Sanctions compliance. Upon request, the Vendor will immediately provide to Ipsos such records and any other information requested by Ipsos, enabling it to verify the Vendor's compliance with this Section 4.2. and Sanctions.

4.2.5. The Vendor: (i) gives the warranties contained in Section 4.2.1 in respect of any subcontractors used in the performance of this Agreement and any related Purchase Orders, as at the date it first uses such subcontractors; (ii) shall impose obligations equivalent to those it has accepted in this Section 4.2. on its subcontractors used in the performance of this Agreement and any related Purchase Orders; and (iii) shall, if so requested by Ipsos, at any time replace any of its subcontractors used in the performance of this Agreement and any related Purchase Orders if the subcontractor is, or is about to become, a Sanctioned Person, contravenes Sanctions, or does anything that could reasonably be expected to result in any of the foregoing.

4.2.6. The Vendor shall promptly notify Ipsos in writing if (i) it becomes aware of any breach or suspected breach of this Section 4.2, or (ii) at any time during the term of this Agreement there is any fact or circumstance that would affect the Vendor's compliance with this Section 4.2., including due to any relevant activities by third parties, such as subcontractors. Vendor shall provide all information about such fact or circumstance or about the actual or suspected breach to Ipsos as Ipsos requires to comply with its obligations to any Sanctions Authority or otherwise reasonably requests.

4.2.7. If at any time during the term of this Agreement the Vendor (i) is, or is about to become, a Sanctioned Person; (ii) has breached, or is in breach of, Sanctions; or (iii) is, or has been, otherwise in breach or non-compliance with this Section 4.2., Ipsos may, in its absolute discretion and without affecting any other right or remedy available to it, terminate this Agreement and any Purchase Order with immediate effect by giving notice to the Vendor, including at any time during or following a suspension of the parties' obligation under Section 15. The Vendor will have no claim against Ipsos in connection with the termination of the Agreement and any Purchase Orders in accordance with this Section.

5. Confidentiality. "Confidential Information" shall mean all information relating to the intellectual property and business practices of either party including, without limitation: (i) information relating to research and development, tools, techniques, methodologies, processes, lessons learned, models, know-how, algorithms, intellectual property rights, trade secrets, specifications, computer programs and software; and (ii) business plans, financial information, products, services, costs, sources of supply, strategic, advertising and marketing plans, customer lists, pricing methods, project proposals, personnel, and business relationships, including, without limitation, any information relating to the business or intellectual property of Ipsos' end clients, (iii) Ipsos Data and Outputs) and (iv) any request for proposal or request for information communicated by Ipsos and these Terms.

5.1. Neither party receiving Confidential Information from the other party shall (i) use Confidential Information received from the other party under this Agreement for any purpose other than to fulfill its obligations under this Agreement; (ii) disclose such Confidential Information to any third party, except for those of its employees with a need to know the information in order to perform their obligations hereunder, and provided that they are made aware of and agree to be bound by the obligations of confidentiality contained herein or are bound by a similar written agreement containing terms regarding confidentiality that are at least as strict as those set forth herein. For the avoidance of doubt: Subcontractors of Vendor are third parties. Confidential Information shall not be disclosed to subcontractors, unless Ipsos has previously agreed in writing, and provided that such subcontractors are made aware of and agree to be bound by the obligations of confidentiality contained herein. The receiving party further agrees to use the same degree of care in safeguarding the Confidential Information as it uses for its own information, but in no event less than a reasonable degree of care. The confidentiality obligations herein shall survive any expiration or termination of this Agreement. Ipsos expressly points out to Vendor that unauthorized disclosure of Confidential Information, in particular professional secrets, social data, bank secrets etc., is punishable by fine or imprisonment.

5.2. The obligation of confidentiality, however, shall not apply to information which: (i) is at the time of receipt or dissemination, or thereafter becomes, generally available to the public other than through a breach of this Agreement by the receiving party; (ii) the receiving party possessed at the time of receipt thereof from the disclosing party, and was not acquired from the disclosing party; (iii) is acquired or rightfully received without confidential limitation by the receiving party from a third party; (iv) is independently

developed by the receiving party without breach of this Agreement; or (v) is required to be disclosed pursuant to court order or applicable law, provided that the receiving party first gives the disclosing party reasonable notice of such court order or law and an opportunity to oppose or attempt to limit such production.

5.3. Nothing in this Agreement is intended to grant any rights to Vendor under any patent, copyright, trademark, trade name or other proprietary right of Ipsos, nor shall this Agreement grant Vendor any rights in or to the Confidential Information. Vendor shall not reverse-engineer, decompile, or disassemble any products, prototypes, software or other tangible objects that embody the Confidential Information nor shall Vendor remove, overprint or deface any notice of confidentiality, copyright, trademark, logo, legend or other notices of ownership or confidentiality from any originals or copies of Confidential Information it obtains from Ipsos.

5.4. Upon completion of the Services or the disclosing party's earlier written request, the receiving party shall at disclosing party's option either: (i) return disclosing party's Confidential Information, in whatever form held by the receiving party, or (ii) certify in a writing signed by a duly authorized officer or representative of the receiving party that such Confidential Information, in whatever form held, has been destroyed. Notwithstanding the foregoing, the parties acknowledge that Confidential Information provided in electronic format (e.g. e-mail but not including any file transfer format) may be copied by the receiving party as part of its normal back-up procedures and as such copies cannot be destroyed or returned to the disclosing party. Each party agrees that it shall a) not access or utilize such copies following receipt of a request to return or destroy Confidential Information from the disclosing party other than for restoration purposes and shall delete any Confidential Information following such restoration and b) the receiving party may retain one copy of the Confidential Information in its legal archives solely for the purpose of determining its obligations hereunder.

6. Personal Data Protection.

Where Ipsos is acting as a controller or processor and Vendor is acting as a processor or sub-processor respectively (as each are defined in the GDPR), Section 6.1 applies. In case Vendor is acting as a controller and Ipsos as a processor, Section 6.2 applies. However, expressions defined in Section 6.1 equally apply to clause 6.2.

6.1. Vendor acting as Ipsos' Processor

If Vendor collects, stores or processes any personal data as defined in Article 4 (1) of the EU General Data Protection Regulation 2016/679 ("**GDPR**") acting as a processor (as defined in the GDPR) in connection with the Services ("**Personal Data**"), Vendor hereby undertakes to protect and safeguard such Personal Data from unauthorized use or access, loss, destruction, theft or disclosure in a manner that meets or exceeds the "**Technical and Operational Measures (including Security Requirements)**" set forth in **Annex 2.** Vendor will not keep the Personal Data on any removable device unless that device is protected by being fully encrypted to a minimum standard of 256-bit AES, the use of the device is necessary for the provision of the Services and an audit trail showing upon which removable device(s) the Personal Data are held is maintained.

Vendor shall use, protect and disclose any Personal Data collected, stored, processed or disclosed strictly in accordance with the provisions of this Agreement and the "**Data Protection Legislation**" which includes all applicable law, rules and regulatory requirements in relation to the processing of Personal Data in any relevant country, including, but not limited to the GDPR, any EU member state or all related national laws, **UK data protection laws** (including the UK GDPR) and any other applicable data protection legislation as amended, superseded or replaced from time to time.

Vendor shall always cooperate with Ipsos and assist Ipsos in complying with Data Protection Legislation, notably by supplying to Ipsos any information required by Ipsos to comply with any filing obligations or other formalities (including but not limited to any data protection impact assessments, transfer impact assessments or legitimate interest assessments), or by making available to Ipsos all information necessary to demonstrate its compliance with the obligations of the Agreement. In all cases, Vendor shall not communicate with any regulator without the express consent of Ipsos, unless legally required.

Vendor undertakes to notify Ipsos immediately and in any event no later than twelve (12) hours upon discovery of any actual or suspected breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed ("**Personal Data Breach**"). Vendor shall:

(i) deliver to Ipsos a written detailed report regarding the nature of the Personal Data Breach, the categories and the approximate number of the Personal Data affected no later than 24 hours after becoming aware of any actual or suspected security breach. Ipsos has the right to request any additional information.

(ii) proceed forthwith (including as Ipsos may direct), at no cost to Ipsos to: (a) mitigate any adverse impact or other harm to Ipsos and any affected data subjects resulting from such Personal Data Breach; and (b) prevent similar Personal Data Breaches from occurring in the future. The Vendor will keep Ipsos fully informed of all stages of its investigation and all actions taken as a result thereof; and

(iii) not without the prior agreement of Ipsos communicate with any authority or other external party concerning the Personal Data Breach, other than as may be legally required.

Vendor undertakes to co-operate with Ipsos to help regain possession (if lost) of such Personal Data and to prevent its further unauthorized use and/or disclosure. Vendor hereby undertakes to immediately notify Ipsos if it has a reasonable belief that it or any other person has contravened, or is likely to contravene, any provision of the Agreement related to Personal Data or Data Protection Legislation.

Vendor shall not retain Personal Data longer than the duration of retention agreed with Ipsos and, in any case, shall not retain those data longer than the authorized duration set forth in the Purchase Order unless if it is required to retain their information to comply with applicable tax/revenue laws or during a dispute resolution procedure, or its obligations to prove consent given. If no duration is set, then the retention duration shall be limited to the duration of the Purchase Order.

Where the Vendor is processing the Personal Data in a country or supra-national region other than that where the Ipsos party is located, the parties agree that the relevant EU standard contractual clauses, as approved by Commission Decision 2021/915, and the UK Addendum ("**SCC**") as set out at SCC Modules 2 & 3 are incorporated into this Agreement (**Annex 2-A "SCC Module 2" and Annex 2-B ("SCC Module 3").** Where Ipsos is acting as controller and Vendor as processor, Module 2 (**Annex 2-A "SCC Module 2")** shall apply. Where Ipsos is acting as processor and Vendor as sub-processor, Module 3 shall apply. The parties undertake to execute and do all such further things as may be necessary to comply with Data Protection Legislation including, but not limited to, the execution between the parties of appropriate other contractual clauses and all subsequent formalities (if any) as required under Data Protection Legislation or the SCC.

Unless applicable Data Protection Legislation allows the transfer or transfer to a sub-processor or to any third party (including for processing, hosting or granting remote access purposes when duly authorized by Ipsos) of Personal Data to a country or supra-national region outside the country or supra-national region where processing under this Agreement has been agreed, Vendor shall not transfer the Personal Data without the prior written consent of Ipsos. If Ipsos grants such written consent to transfer the Personal Data outside such countries or regions, the Vendor (including any relevant recipient of the Personal Data) shall (a) comply with the obligations defined by the Data Protection Legislation by providing an adequate level of protection to any of the Personal Data that is transferred in the countries agreed by Ipsos and providing evidence of the adequate level of protection to Ipsos; (b) comply with any reasonable instructions notified to it by Ipsos and (c) undertake to execute and do all such things as may be necessary to comply with Data Protection Legislation including, but not limited to, the execution between the Parties of appropriate SCC.

Unless it receives Ipsos' prior written consent, Vendor (i) will not access or use any Ipsos data or Personal Data other than as necessary to facilitate the Services provided hereunder; and (ii) will not give any third-party access to Ipsos data or Personal Data without Ipsos' prior written consent.

6.2. Vendor acting as Controller

If Vendor provides any Personal Data acting as a controller (as defined in the GDPR), the parties agree that the "**Technical and Operational Measures (including Security Requirements)**" set forth in **Annex 2** and to be applied *mutatis mutandis* constitute appropriate technical and operational measures for the purposes of any applicable Data Protection Legislation. Ipsos will not keep the Personal Data on any removable device unless that device is protected by being fully encrypted to a minimum standard of 256-bit AES, the use of the device is necessary for the provision of the Services and an audit trail showing upon which removable device(s) the Personal Data are held is maintained.

Ipsos shall use, protect and disclose any Personal Data collected, stored, processed or disclosed strictly in accordance with the provisions of this Agreement, any Purchase Order and the Data Protection Legislation.

Ipsos shall always cooperate with Vendor and assist Vendor in complying with Data Protection Legislation, notably by supplying to Vendor any information required by Vendor to comply with any filing obligations or other formalities (including but not limited to any data protection impact assessments, transfer impact assessments or legitimate interest assessments), or by making available to Vendor all information necessary to demonstrate its compliance with the obligations of the Agreement. In all cases, Ipsos shall not communicate with any regulator without the express consent of Vendor, unless legally required.

Ipsos undertakes to notify Vendor immediately and in any event no later than twelve (12) hours upon discovery of any actual or suspected Personal Data Breach. Ipsos shall:

(i) deliver to Vendor a written detailed report regarding the nature of the Personal Data Breach, the categories and the approximate number of the Personal Data affected no later than 24 hours after becoming aware of any actual or suspected security breach. Vendor has the right to request any additional information.

(ii) proceed forthwith (including as Vendor may direct), at no cost to Vendor to: (a) mitigate any adverse impact or other harm to Vendor and any affected data subjects resulting from such Personal Data Breach; and (b) prevent similar Personal Data Breaches from occurring in the future. Ipsos will keep Vendor fully informed of all stages of its investigation and all actions taken as a result thereof; and

(iii) not without the prior agreement of Vendor communicate with any authority or other external party concerning the Personal Data Breach, other than as may be legally required.

Ipsos undertakes to co-operate with Vendor to help regain possession (if lost) of such Personal Data and to prevent its further unauthorized use and/or disclosure. Ipsos hereby undertakes to immediately notify Vendor if it has a reasonable belief that it or any other person has contravened, or is likely to contravene, any provision of the Agreement related to Personal Data or Data Protection Legislation.

Ipsos shall not retain Personal Data longer than the duration of retention agreed with Vendor and, in any case, shall not retain those data longer than the authorized duration set forth in the Purchase Order unless if it is required to retain their information to comply with applicable tax/revenue laws or during a dispute resolution procedure, or its obligations to prove consent given. If no duration is set, then the retention duration shall be limited to the duration of the Purchase Order.

Where Ipsos is processing the Personal Data in a country or supra-national region other than that where the Vendor is located, the parties agree that the SCC as set out at SCC reverse Module 2 SCC as set out in **Annex 2-C "SCC Module 2 Reverse")** are incorporated into this Agreement and undertake to execute and do all such further things as may be necessary to comply with Data Protection Legislation including, but not limited to, the execution between the parties of appropriate other contractual clauses and all subsequent formalities (if any) as required under Data Protection Legislation or the SCC.

Unless applicable Data Protection Legislation allows the transfer or transfer to a sub-processor or to any third party (including for processing, hosting or granting remote access purposes when duly authorized by Vendor) of Personal Data to a country or supra-national region outside the country or region where processing under this Agreement has been agreed, Ipsos shall not transfer the Personal Data without the prior written consent of Vendor. If Vendor grants such written consent to transfer the Personal Data outside such countries or supra-national regions, Ipsos (including any relevant recipient of the Personal Data) shall (a) comply with the obligations defined by the Data Protection Legislation by providing an adequate level of protection to any of the Personal Data that is transferred in the countries agreed by Vendor and providing evidence of the adequate level of protection to Vendor; (b) comply with any reasonable instructions notified to it by Vendor and (c) undertake to execute and do all such things as may be necessary to comply with Data Protection Legislation including, but not limited to, the execution between the Parties of SCC.

Unless it receives Vendor' prior written consent, Ipsos (i) will not access or use any Vendor data or Personal Data other than as necessary to facilitate the Services provided hereunder; and (ii) will not give any third-party access to Vendor data or Personal Data without Vendor' prior written consent.

7. **Indemnification.** Each party shall indemnify, defend and hold harmless the other party, its affiliated companies and each of its respective officers, directors, employees and agents from and against all claims and resulting liabilities, losses, damages, costs and expenses of any kind, including reasonable attorneys' fees, initiated by or on behalf of third parties (including from Ipsos' end client and Vendor's subcontractors) to the extent arising out of any acts or omissions of a party or any breach or violation by a party of its representations and warranties or other terms of this Agreement.

8. **Limitation of Liability. a)** Neither party shall be liable to the other for lost profits or revenues or other speculative economic loss, including consequential, special, punitive or other similar damages, arising from or related to this Agreement, except with respect to third party indemnification claims (including from Ipsos' end client and Vendor's subcontractors) as specified above in Section 7, Vendor's gross negligence or fraud or willful misconduct and Vendor's breach of its confidentiality and security obligations. b) Ipsos shall not be liable for damages caused by simple negligence, except in the case of injury to life, body, health or essential contractual obligations. Essential contractual obligations are those whose fulfillment characterizes the Agreement and on which the other contractual party may rely. In the event of property damages or financial losses caused by a breach of such essential contractual obligations due to simple negligence, Ipsos shall only be liable for the foreseeable damage typical for the Agreement. The aforementioned limitations of liability shall also apply in favor of the legal representatives, directors, employees, workers and vicarious agents of Ipsos. However, the aforementioned limitations of liability shall not apply to any liability prescribed by law or to liability arising from a warranty or in the event of intent or gross negligence.

9. **Ownership of Work Product and Use of Artificial Intelligence.**

9.1. Each party will at all times maintain sole and exclusive ownership of their respective intellectual property rights and data. Each party will agree not to reverse assemble, reverse compile, or otherwise translate the other party's intellectual property and software they own except as expressly permitted by the other party in connection with the Services under this Agreement.

9.2. Ipsos shall own all ideas, designs, concepts, materials, reports, data, analyses, inventions, discoveries, improvements, and processes created or developed by Vendor which result from the performance of the Services, including, without limitation, all deliverables identified in the Purchase Order and all intellectual property rights therein (collectively, the **"Work Product**"). The Work Product shall be considered "works made for hire" in accordance with United States copyright law or any other applicable law. In the event that such works are determined not to constitute "works made for hire" as a matter of law, Vendor hereby irrevocably assigns to Ipsos all of its right, title and interest in and to the Work Product, including, without limitation, all related intellectual property rights and all applications therefor. The price corresponding to such present assignment is included in the fees paid by Ipsos under this Agreement or the relevant Purchase Order. Upon Ipsos' request, Vendor will execute and deliver to Ipsos all documents necessary to perfect Ipsos' right, title and interest in and to the Work Product. To the extent any assignment is not permitted by applicable laws, Vendor, or its employees and approved subcontractors, as applicable, shall grant Ipsos and its Affiliates an exclusive, transferable, sublicensable, perpetual, worldwide, unlimited license in the Work Product in any and all media, whether existing or hereafter developed, including the exclusive right to copy, reprint, rework, multiply, modify and create derivative works of the Work Product. Ipsos shall not pay any separate compensation for such license. Without limiting the generality of the foregoing, if Vendor enhances, modifies or creates derivative works of any Work Product, any such copies, modifications and/or derivative works shall remain or be the sole and exclusive property of Ipsos.

Notwithstanding the foregoing, Vendor will retain ownership of Vendor's technologies and other intellectual property rights in existence prior to the commencement of Services hereunder or developed independently of the Services hereunder, unless created expressly for the performance of the Services or the benefit of Ipsos. Vendor grants to Ipsos and its Affiliates a non-exclusive, royalty free, perpetual, irrevocable, world-wide license to use and copy any such intellectual property that is incorporated into the Work Product or the Services to the extent necessary to use the Work Product and the Services for Ipsos' business purposes.

9.3. Notwithstanding anything in this Agreement to the contrary, Vendor represents, warrants and covenants that it shall not (and shall allow any third party to) utilize any AI Models (as defined below) to ingest, train or fine-tune on, analyze, process or otherwise use any content, information, data or other material provided or made accessible to Vendor by, or belonging to, Ipsos or Ipsos' clients, whether or not aggregated, anonymized or masked (collectively, "**Ipsos Data**"), without Ipsos prior express written consent.

"AI Model(s)" means any software, system, product or service that utilizes artificial intelligence, machine learning, statistical language modelling, neural networks and/or other similar technologies (whether now known or hereafter developed).
If and to the extent Ipsos authorizes Vendor to utilize (or to permit a third party to utilize) Ipsos Data in connection with any AI Model(s), Vendor represents, warrants and covenants that Vendor will only utilize (or permit the third party to utilize, as applicable) as specifically authorized in respect of the Ipsos Data, form (e.g., aggregated, anonymized or marked), manner, purpose or purposes, specific AI Model or AI Models, and in accordance with any other parameters (e.g., duration) stipulated by Ipsos. If the foregoing results in any new content, information, data or other material ("**Output**"), Vendor agrees that Ipsos owns all right, title and interest in and to such Output. To the extent that any such right, title or interest vests in Vendor (or the authorized third party), Vendor hereby assigns (or shall cause the third party to assign, as applicable) all of the same to Ipsos.

Ipsos Data and Outputs (if any) are Ipsos' Confidential Information.

Vendor shall, in any event, within thirty (30) days of the date of termination of a Purchase Order or expiry of the Services (a) return a copy of all Ipsos data or provide a self-service functionality allowing Ipsos to do the same; and (b) delete all other copies of Ipsos data processed by Vendor or any sub-processors.

9.4 **Ownership of Vendor Sample Sources.** Ipsos agrees – unless otherwise agreed upon – that Vendor's respondent community and the identities of the respondents are and shall be solely owned by Vendor and constitute its confidential and proprietary information. Ipsos will never try to identify data subjects, which are only described by ID or numbered list.

10. **Audit.** During the Term and for two (2) years thereafter, Ipsos or its designated representatives or independent audit firm retained by Ipsos may, on reasonable notice and at any reasonable time, audit the Vendor's records, books, data, Personal Data, management practices and the data security practices of Vendor or of any sub processor or subcontractor of Vendor to ensure compliance with this Agreement. Vendor will make available to Ipsos all necessary information (such as Vendor's audit reports and the audit reports of its sub-processors/subcontractors, if any) and allow Ipsos, Ipsos' end clients, a Data Regulator Authority to conduct an audit (including inspections) including an access to Vendor's (and its sub-processor's/subcontractors) premises, facilities, equipment, information and records, and to provide such

contributions as may be reasonably required by Ipsos to demonstrate and enable Ipsos or any third party or authority to verify Vendor's and/or its sub-processor's/subcontractors compliance with the Agreement and the applicable Data Protection Legislation.

11. **Non-Solicitation of Employees and Non-Solicitation of Clients:**
11.1. During the Term and for a period of twelve (12) months thereafter, Vendor will not, either for itself or for a third party, solicit or hire any of Ipsos' employees or contractors or induce any of them to terminate or breach an employment, contractual or other relationship with Ipsos or to devote less than their full best efforts to the interests of Ipsos provided, however, that Vendor will not be prevented from making general solicitations of employment through newspaper or similar advertisements, or through search firms, provided such solicitations are not directed to Ipsos' employees.

11.2. During the Term and for a period of twelve (12) months thereafter, Vendor will not, either for itself or for a third party, directly or indirectly, encourage or assist any person or entity to (i) solicit the business of or directly perform any competing services for actual or prospective clients of Ipsos (x) as to which Vendor performed Services or had direct contact in connection with Vendor's engagement with Ipsos or (y) as to which Vendor had access to client confidences or client confidential information during the course of Vendor's relationship with Ipsos or (ii) to encourage or induce any such client to cease doing business with, or reduce the extent of its business dealings with, Ipsos, and Vendor shall refer all opportunities relative to such clients exclusively to Ipsos.

12. **Insurance.** At all times during the course of performing any services for Ipsos, Vendor will maintain insurance from reputable insurers of the types of insurances (including their amounts) listed in **Annex 3**. In the event of damage for which the Vendor is responsible, the Vendor shall do everything in its power to ensure that Ipsos (or Ipsos' client) is compensated for its damage. The Vendor undertakes to assign the claims arising from the respective insured event to Ipsos. Upon the request of Ipsos, Vendor will promptly furnish Ipsos with certificates confirming such insurance coverage.

13. **No Subcontracting or Sub-processing.** Vendor will not engage a subcontractor or a sub-processor and/or transfer Personal Data to any subcontractor or subprocessor without Ipsos' prior specific consent. To enable Ipsos to provide its consent, Vendor will ensure that it and the sub-processor or the subcontractor will enter into a written contract on terms which provide that the sub-processor or subcontractor has the same *mutatis mutandis* obligations as Vendor as are set out in the Agreement. Vendor shall disclose to Ipsos the whole subcontracting chain (including all the details of each subcontractor or sub-processor and any information requested by Ipsos) when Vendor is authorized by Ipsos to subcontract a portion or the whole Services to a third party.

Ipsos has the right to require the replacement of Vendor's personnel or of any subcontractor who is unqualified or presents a security risk and for any lawful or legitimate reason.

14. **Assignment, Transfer and Change of Ownership.**

This Agreement will be binding upon and will inure to the benefit of the parties and their permitted successors and assigns, provided that Vendor shall not assign or transfer this Agreement without the express prior written consent of Ipsos.

Each time there is a foreseeable evolution of the structure of a change of ownership of Vendor, specifically when such change of ownership includes an Ipsos competitive entity, Vendor shall promptly notify Ipsos in priority and in writing of such changes. Ipsos will keep strictly confidential any information provided by Vendor pursuant to this Section.

15. **Force Majeure**. Neither party shall be deemed to be in breach of this Agreement for any failure or delay in performance caused by a "Force Majeure Event, provided that such party (i) timely gives notice of the Force Majeure Event to the other party after its occurrence, (ii) uses its reasonable efforts (including executing any disaster plan) to overcome, mitigate and remove the cause of the event preventing or delaying performance, and (iii) continues the performance of all its obligations under this Agreement that are not prevented or delayed. Ipsos shall not be required to pay fees and shall receive a prorated refund for any prepaid fees, during any such failure to perform by Vendor. If and to the extent any Force Majeure Event has prevented or is reasonably expected to substantially prevent the provision of the Services or for a period of more than thirty (30) calendar days, Ipsos may terminate this Agreement fully or partly upon written notice. **"Force Majeure Event"** means any circumstances beyond the reasonable control of a party (and unknown to such party at the date of this Agreement) including but not limited to acts of God, fire, pandemic, explosion, adverse weather, flood, terrorism, civil commotion, war and riots. Any failure of Vendor's subcontractors shall not be considered as a Force Majeure Event unless caused by a Force Majeure Event.

16. **Governing Law and Venue.** This Agreement shall be governed by and interpreted in accordance with the laws of the country where the Ipsos entity (or Affiliate) who placed the Services under a Purchase Order is located, without reference to its principles of conflict of law (except for the case, where the Ipsos entity (or Affiliate) who placed the Services under a Purchase Order is located in the United States, then this Agreement shall be governed by and interpreted in accordance with the laws of the State of New York, USA). For all the disputes arising out of this Agreement or relating to the Services, each party hereto consents exclusively to subject matter and *in personam* jurisdiction and venue of federal or state courts in the country or the State where the Ipsos entity (or Affiliate) who placed the Services under a Purchase Order is located (except for the case, where the Ipsos entity (or Affiliate) who placed the Services under a Purchase Order is located in the United States, each party hereto consents exclusively to subject matter and *in personam* jurisdiction and venue of federal or state courts in New York, USA).

17. **Independent Contractors.** Vendor is an independent contractor of, and not an employee, agent or authorized representative of, Ipsos. No agency, partnership, joint venture, employer-employee relationship, or other business combination between Vendor and Ipsos is intended or created by this Agreement. Vendor will be responsible for payment and/or withholding of all income, social security, unemployment compensation, workers compensation, and other employment-related taxes pertaining to Vendor and its employees, and Ipsos will have no such responsibilities, nor will Ipsos be responsible for any health, life, disability or other benefits for Vendor or its employees. Vendor will have no authority to bind Ipsos to any undertaking or agreement with any third party.

18. **Injunctive Relief.** Vendor acknowledges that, in view of the nature of the business in which Ipsos is engaged, irreparable injury to Ipsos could result should Vendor violate the confidentiality and non-solicitation provisions set forth herein. Vendor therefore agrees that in the event of any actual or threatened violation of those Sections, Ipsos will, in addition to all other rights and remedies available to it, at law or otherwise, be entitled to an immediate injunction to be issued by any court of competent jurisdiction restraining Vendor from committing such violation, together with reimbursement of any costs and attorneys' fees incurred by Ipsos to enforce this Agreement.

19. **ESG – Climate Action.**

ESG and climate action. Vendor acknowledges that Ipsos' intention in the fulfilment of Vendor's obligations under this Section is to minimize its negative impact on climate change and biodiversity, and to reduce its Product Carbon Footprint to help Ipsos to achieve its ESG objectives. Vendor shall comply with Ipsos ESG's objectives as described in **Annex 4**.

20. **Healthcare - Pharmacovigilance.** Where the Services relate to healthcare and/or pharmaceutical market research and unless agreed otherwise, Vendor agrees to comply with the Healthcare Compliance document attached at **Annex 5**.

21. **Entire Agreement - Non-Waiver - Severability.** The Agreement contains the sole and entire agreement between the parties with respect to its subject matter and shall not be modified except by a written instrument signed by Ipsos and Vendor. The non-invoking by one of the parties of a breach of the other party under the terms of this Agreement shall not be construed as waiver in this regard and the relevant party shall not be barred from later invoking of the same breach or any other breach during the Term. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected and those provisions shall remain in full force and effect. If a court or other decision-maker should determine that any provision of this Agreement is overbroad or unreasonable, such provision shall be given effect to the maximum extent possible by narrowing or enforcing in part that aspect of the provision found overbroad or unreasonable.

22. **Notices:** All notices and other communications under these Terms shall be given in writing to the parties by e-mail or at the addresses appearing in the Purchase Order, or to such other address specified in writing to the notifying party after the date of the Purchase Order and shall be deemed given on the date delivered in person, or on the next business day following delivery by a reputable overnight courier for next day delivery, or if by e-mail with a return receipt requested.

23. **Specific Purchasing Terms for IT Services:** If the Services covered by a Purchase Order are related to a software licenses and any related IT services ("**IT Services**"), such IT Services shall be governed by the specific terms set forth in **Annex 6** **("Specific Purchasing Terms for IT Services**") in addition to the Ipsos Purchasing Terms.

ANNEXES ATTACHED TO IPSOS PURCHASING TERMS

Annex 1: Ipsos Supplier Code of Conduct

Annex 2: Technical and Operational Measures (including Security Requirements)

Annex 2-A: SCC Module 2

Annex 2 – B: SCC Module 3

Annex 2 -C: SCC Module 2 Reverse

Annex 3: Insurances policies required by the Vendor

Annex 4: ESG – Climate Action

Annex 5: Healthcare Compliance

Annex 6: Specific Purchasing Terms for IT Services

ANNEX 1
IPSOS SUPPLIER CODE OF CONDUCT

1. Summary

Ipsos is committed to complying with all applicable laws, regulations, national and international conventions, and best practices with regards to ethics, social responsibility, and protection of the environment, including in particular the fight against climate change.

Ipsos expects its suppliers to comply with applicable laws and the ethical practices and principles that are contained in this Supplier Code of Conduct (this "Code"). Ipsos requires its suppliers to adhere to (1) this Code, (2) the principles stipulated in the Conventions of the International Labour Organization, which can be accessed here: http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html, the Universal Declaration of Human Rights, and the United Nations Global Compact, and (3) the Duty of Care obligations set out in the French Law N° 2017-339 as of today and as updated from time to time. Each supplier is also responsible for ensuring that its own, personnel, agents, subcontractors and consultants (collectively referred to as "Supplier(s)") do the same, thus passing on these standards along their own supply chain".

When national legislation or other applicable regulations address the same issue as this Code, the highest standards or most restrictive provisions shall apply.

Supplier acknowledges that the provisions of this Code are in addition to, and not in lieu of, the provisions of any legal agreement or contract between a Supplier and an Ipsos entity.

If this Code is violated by a Supplier, Ipsos reserves the right to review the business relationship with such Supplier and possibly terminate such relationship, without prejudice to Ipsos' other rights and remedies. This is true even if there are no written arrangement or undertaking or contracts between Ipsos and the Supplier.

The agreements with the Supplier shall contain the required provisions to ensure that a Supplier complies with this Code.

- Supplier warrants and represents that Supplier and its Subcontractors will comply with this Code attached to the relevant agreement,
- Ipsos can terminate the agreement with Supplier in case of any breach of Supplier or its Subcontractors of this Code.

If not, each Supplier should sign, date and acknowledge that Supplier has received, read, and agrees to comply with the Code.

2. Ipsos commitments to its suppliers

A. Ensure a fair selection

Ipsos will ensure fair competition and a fair selection process for Suppliers. It generally aims to have a diverse set of suppliers, reflecting the diversity of businesses and of the population of the countries where they operate, as long as they meet Ipsos' business needs.

B. Guarantee of fair financial treatment

Ipsos pays its Suppliers in accordance with all legal obligations, and in compliance with any applicable rules and regulations.

C. Reduce the risk of mutual dependence

Ipsos seeks to avoid technical monopolies and to reduce the risk of mutual dependence in its relationships with its Suppliers. Accordingly, Ipsos makes every effort to diversify its sources of supply and require our Suppliers to commit to doing the same.

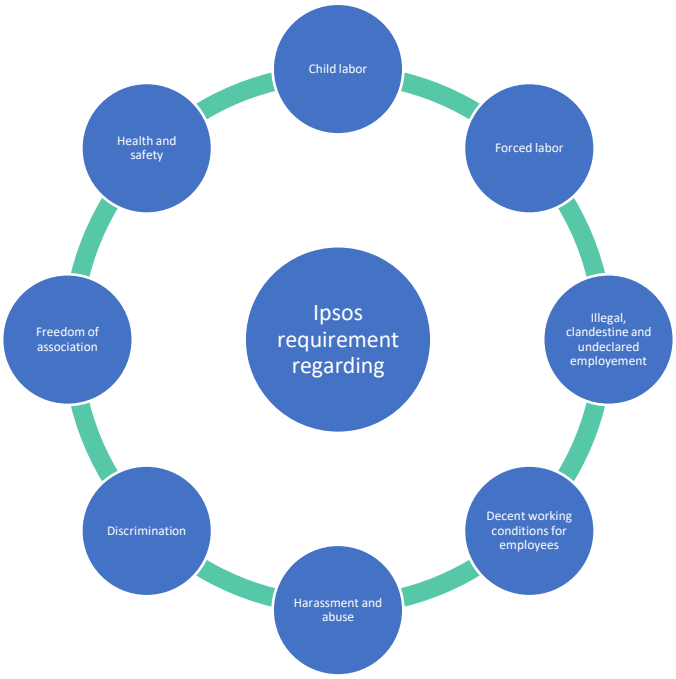
D. Adopt a common corporate social responsibility approach with supplier

Ipsos strongly prefers to work with Suppliers who have adopted a similar approach to its own in terms of Environment, Social and Governance (ESG) commitment and Corporate Social Responsibility, particularly those who have taken concrete steps to reduce their environmental impact (carbon emissions, consumption of water, energy, raw materials) and improve society (the working conditions of employees, diversity within their company, the consequences of their activity on society in general).

3. Commitments from Ipsos suppliers

A. Labor standards and social responsibility

This Code outlines the values that both individual employees and the collective body at Ipsos should adhere to. Ipsos firmly believes that the key to its growth lies in the trust and respect that exists between Ipsos and its employees, as well as among the employees themselves and all Ipsos' suppliers Ipsos is working with. It is the responsibility of each Ipsos' suppliers to ensure that they follow this Code in their daily tasks.



Ipsos requires its Suppliers to exhibit exemplary social responsibility in their conduct:

- Prohibition of child labor: Work by children under the age of 16 is strictly prohibited, even if permitted by law. In countries where local laws set a higher minimum age for child labor, the higher age is applicable.
- Prohibition of forced labor: Any use of forced labor, slavery, servitude or trafficking in human beings by our Suppliers, as well as withholding identification documents or work permits, is strictly prohibited.
- Prohibition of illegal, clandestine and undeclared employment**:** Our Suppliers are required to comply with all applicable regulations to prevent illegal, clandestine and undeclared employment.
- Fair pay: We expect our Suppliers to pay their employees a fair wage that allows them to live decently.
- Decent working conditions for employees: We expect our suppliers to guarantee decent working conditions for their employees, including appropriate working time.
- Prohibition of harassment and abuse: We expect our Suppliers to treat their workers with respect and dignity.
- Prohibition of discrimination: We expect our Suppliers to treat all workers equally and fairly. Our Suppliers may not engage in any kind of discrimination – in particular, with regards to wages, hiring, access to training, promotion, maternity protection and dismissal – based on sex, race or ethnic origin, religion, age, disability, sexual orientation, political affiliation, union membership, nationality, gender identity or social background.
- Freedom of association: We require our Suppliers to respect and recognize the right of workers to negotiate collectively, and to create or join labor organizations of their choice, without any sanction, discrimination or harassment.
- Ensuring health and safety: Our Suppliers are expected to provide their workers with a safe and healthy workplace environment in order to avoid accidents or bodily injuries which may be caused by, related to, or result from their work, including during the operation of equipment or during work-related travel.

B. Environmental regulations and protection

Ipsos encourages concrete measures to protect the environment, including cooperation with its Suppliers to ensure application of best practices throughout the supply chain.

Ipsos encourages initiatives by its Suppliers to reduce their environmental impact, notably through the use of "green" technologies.

In particular, Ipsos expects its suppliers to work on reducing their carbon emissions, ideally by taking a pledge to reaching Net Zero by 2050 and joining one of the different recognized schemes and initiatives in this field – like the Science-Based Targets Initiative (SBTi).

Ipsos requires its Suppliers to respect local and international environmental regulations and standards.

Ipsos' Suppliers are expected to make regular improvements in the environmental performance of their sites and production resources, in particular through proper waste management; elimination of air, water and soil pollution; appropriate handling and disposal of any hazardous chemicals and any other dangerous or polluting material they may use; reduction of greenhouse gas emissions with an emphasis on use of renewable energy, and a reduction of water and energy consumption.

C. Business integrity requirements

Ipsos requires its Suppliers to conduct their business activities with exemplary integrity:

- Legal requirements: We expect our Suppliers to conduct their business in full compliance with local, national and international laws. In particular, we expect them to comply with tax legislations applicable to them, as well as with export controls and economic sanctions as applicable.
- Financial integrity: Accurate and reliable financial and business records are of critical importance in meeting Ipsos' financial, legal, and business obligations. Suppliers should not have any false or inaccurate entries in the accounting books or records related to Ipsos for any reason. Suppliers' business records must be retained in accordance with record retention policies and all applicable laws and regulations.
- Prohibition of all forms of corruption: We expect our Suppliers to respect all applicable laws concerning corruption, extortion, and bribery and to take appropriate measures to prevent, detect and sanction the foregoing.
- Prevention of conflicts of interest: We require our Suppliers to comply with all applicable laws concerning conflicts of interest and to make every effort to prevent situations that may create a conflict or appearance of conflict of interest within the scope of their business relationship with Ipsos.
- Prohibition of money-laundering: Money-laundering can occur where an action is taken to mask the true origin of money or assets that are connected to criminal activity. We require our Suppliers to commit to taking all appropriate measures to prevent their operations from being used as vehicles for money-laundering.
- Respect of anti-trust and competition: Our Suppliers must comply with all applicable anti-trust and competition laws. This includes prohibiting abuse of a dominant market position, not engaging in concerted practices and not entering into unlawful agreements with competitors. Antitrust or competition laws may differ from country to country but generally prohibit actions that unreasonably restrain trade or reduce competition.
- Protection of personal information: We require our Suppliers to comply with all applicable laws and regulations concerning the protection of personal information.

D. Business ethics requirements

- Gifts and invitations: Gifts or invitations may be considered acceptable expressions of courtesy within the context of good business relations if:
    - Limited in scope and value;
    - Given openly and transparently;
    - Permitted under applicable local law;
    - Customary in the location in which they would be given;
    - Provided to reflect esteem or gratitude; and
    - Not offered with an expectation that something will be offered in return.

In some cases, these practices might be subject to anticorruption regulations or other legal requirements, making it essential to be aware of such rules and to fully comply with them.

- Information transparency: Our Suppliers are required to provide clear and accurate information regarding the methods and resources used, production sites and characteristics of the products or services supplied, and to refrain from making any misleading claims.

E. Inspection and Audit

- Inspection: We reserve the right to confirm compliance with these principles and to conduct compliance audits, whether in-person or virtual, of our Suppliers. Our Suppliers must provide all necessary information and facilitate access by representatives of Ipsos seeking to verify compliance with the requirements of this Code. Suppliers must commit to promptly improving or correcting, at its own costs, any deficiencies identified during an audit.
- Accurate books and records and access to information: Our Suppliers are required to keep proper accurate and transparent books and records to demonstrate compliance with this Code. They must provide our representatives with access to these books and records.

F. Reporting and non-compliance with this code

Suppliers are responsible for prompt reporting of actual or suspected violations of applicable law and this Code. This includes violations by any worker or agent or subcontractor acting on behalf of the Supplier. Supplier may report a violation via e-mail using the following address: Supplier_Compliance_&_ESG@ipsos.com. A Supplier's failure to comply with or rectify (within the time period specified by Ipsos), any provision of this Code may result in the termination of any contracts or relationships with such Supplier.

If a Supplier is unable to meet any of this Code's requirements, it should immediately notify Ipsos and submit a corrective action plan to correct the identified deficiencies. Ipsos reserves the right to accept or reject this action plan based upon the appropriateness of the measures and compliance deadlines proposed by the Supplier.

Annex 2
Technical and Operational Measures (including Security Requirements)

Organizational Safeguards

- Vendor must sign a non-disclosure agreement, which must then be co-signed by an IPSOS executive, prior to be granted access to Ipsos data and/or environment
- Vendor has appointed an employee who has data protection and information security responsibilities set out as part of their duties.
- Physical access to the building is limited by various access control mechanisms (for instance key cards) and in most cases entrances to Vendor's offices are staffed by receptionists/security staff.
- Vendor employees are instructed on data protection and information security matters upon commencing employment with Vendor and are subject to confidentiality obligations.
- Employees are not permitted to record Personal Data on a storage medium (e.g. disk) to enable them to re-access the information in premises that are not controlled by Vendor.
- In the event that Personal Data is held in hard copy format, any employees dealing with such Personal Data operate a clear desk policy, so that no Personal Data is left unattended in their absence. Personal Data in hard copy form is stored securely to prevent any unauthorized access.
- A business continuity plan shall be put in place and tested yearly

Information Security Risk Management

- Vendor must periodically assess risk within Information Technology specifically toward assets associated/involved in the services/products delivered to Ipsos. The implemented risk management framework should be in agreement with the requirements of the ISO 27001 & ISO 27002 or ISO 31000.

Information Security Policy

- Vendor must document their Information Security Policies and follow Information Security programs that are based on at least one of the following frameworks:
    - ISO 27001 & ISO 27002 standards
    - NIST 800 Special Security Publications.

- Vendor must map their security program to one of the above security frameworks showing no gaps in their information security program.

Information Security framework

- Vendor must define, document, and assign ownership to oversee development, adoption, enforcement and compliance with Information Security requirements, policies, standards, and procedures.
- Vendor must ensure the assigned role must be of a sufficiently high-level classification in the organization that can be allowed to execute the responsibilities in an effective and independent manner.
- To avoid conflicts of interest, Vendor must ensure this role will not have direct responsibility for information processing and technology operations.

Asset Management

- Vendor must design, document, implement and maintain an asset management process – having in scope the Vendor assets -, having the possibility to map the dependency between Vendor assets and Ipsos assets - including informational assets.
- Vendor must assign designated individual that is responsible for all Vendor Assets that access Ipsos assets and data.
- Vendor must document and implement rules for the acceptable use of assets of third parties, including without limitation, Ipsos assets and data.
- Rules of acceptable use must require that third party assets are not to be used for activities which have been identified as unacceptable conduct.
- Rules of acceptable use must require that third party assets are to be used in a professional, lawful and ethical manner.
- If Vendor connects to or use Ipsos asset(s) (including servers, workstations, infrastructure, internet gateway or network) must abide by all applicable Ipsos terms of use, policies, standards, and procedures.
- Vendor is required to safeguard and use Ipsos assets wisely and will use good judgment and discretion when using Ipsos assets including Ipsos systems, computers, telephones, internet access, email, voice mail, copiers, fax machines, vehicles or other property.
- Vendor must never connect non-Ipsos owned assets to Vendor's network without direct written approval from Ipsos.
- Ipsos must review and approve all requests from any company to connect non-Ipsos owned assets to the Ipsos network.
- Assets that connect to Ipsos network must abide by Ipsos Security Policies, Standards, Operating practices and controls, including, but not limited to configuration, hardening, patching, access control and virus protection processes.

Human Resources Security

Vendor must:

- Ensure all Vendor employees, Vendors, and subprocessors who access Ipsos assets are screened prior to employment. Screening must include criminal, financial, employment background screening processes, while not conflicting with the applicable legislation.
- Have processes in place to periodically screen personnel during employment for anyone who accesses Regulated, Confidential, or Personal information.
- Ensure an Information Security awareness campaign is provided to everyone who has access to Ipsos assets. Campaign must educate personnel of their responsibility to secure Ipsos assets.
- Ensure all user IDs, tokens or physical-access badges are assigned to a unique Vendor employee or Vendor subprocessor.
- Ensure all user/system/service/administrator accounts and passwords are never shared.
- Immediately notify Ipsos in writing if a Vendor employee or subprocessor is not working on the Ipsos account or ID permission must be changed on a Ipsos managed assets and data. Notices must include name, user ID name of any accounts the person had access to or knows the password.

Physical and Environmental Security

Vendor must implement all the necessary information security controls in order to assure that all Vendor assets involved in the services provided to Ipsos as well as any Ipsos assets existing in Vendor custody are protected from:

- Natural disasters,
- Theft, physical intrusion, unlawful and unauthorized physical access,
- Ventilation, Heat or Cooling problems, power failures or outages.

Operations Management

***Network Security*:** Vendor must deploy Data Loss Prevention (DLP) and or intrusion monitoring services at perimeter points where Ipsos regulated, confidential or Personal Data is used.
Vendor must ensure all unnecessary services, ports, and network traffic are disabled on all IT systems that access Ipsos assets.

***System Security*:**
Vendor must have a process for applying and managing security updates, patches, fixes upgrades, (collectively referred to as "Patches") on all Vendor IT systems.

- Vendor must ensure patches that provide security fixes or security updates are tested and deployed within 20-days from the date of release, for all Vendor IT systems that access Ipsos Confidential, Personal, or Regulated Information.
- Otherwise, Vendor must ensure patches are deployed within 30-days from the date of release.
- All exceptions are to be documented while stating the reason for not deploying the mentioned patches.

Vendor must ensure Malware, Virus, Trojan and Spyware protection programs are deployed on all IT systems that access Ipsos assets and data; the mentioned must have the latest and up-to-date manufacture's signatures, definition files, software and patches.
Vendor must ensure all unused or unnecessary software, applications, services, sample/default files and folders are disabled on all IT systems that access Ipsos assets and data.

***Operation Security - Vendor must*:**

- Ensure that any changes to IT systems that are performing work on or for Ipsos do not have any negative security implications.
- Follow documented change management practices and procedures
- Not move or transfer Regulated, Personal or Confidential information to any non-production environment or insecure location.

Disaster recovery

- Vendor has implemented appropriate disaster recovery measures to ensure that the Personal Data it processes can be re-instated in the event of loss or destruction of that data.
- The disaster recovery plan which will implement the disaster recovery measures will define RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives). The RPO and RTO will be communicated inside of the DR Plan to Ipsos within 20 business days of the contract signature.
- Vendor periodically reviews these technical safeguards to ensure their continued suitability in light of the data it processes and technological advances.

Data management

Data Security
Vendor must:

- Use strong encryption key management practices to ensure the availability of encrypted authoritative information
- Encrypt all Ipsos data assets in transmission between Vendor and Ipsos as well as between Vendor and all other third parties when transmitted data is Ipsos data.
- Encrypt Ipsos confidential information at all times; encryption must meet a minimal standard of AES-256-bit encryption.
- In the case that a public/private encryption tool is used, Vendor must take every step to protect the private key.
- When encrypting Ipsos data do not send passwords/passphrases via e-mail or via voicemail
- If a password/passphrase is used in the encryption of the document, communicate the password/passphrase for the encrypted document out of band:
- Face to face
- Live on the telephone

Transferring of Data
Acceptable Methods of Data Transfer:

- Secure File Transfer Protocol (SFTP): SFTP is an encrypted version of FTP that uses SSH to transfer data securely between clients and servers, ensuring the confidentiality and integrity of the data.
- File Transfer Protocol Secure (FTPS): FTPS is an extension of FTP that adds support for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols to encrypt data during transmission.
- Hypertext Transfer Protocol Secure (HTTPS): HTTPS is an encrypted version of HTTP that uses SSL/TLS to secure communication between web servers and clients.
- Virtual Private Network (VPN): A VPN creates a secure, encrypted tunnel between devices, enabling secure data transfer over public networks.
- Encrypted Email: Secure email solutions like PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions) provide end-to-end encryption, ensuring the confidentiality of email communication.
- Encrypted Cloud Storage: Services like Google Drive, Dropbox, or Microsoft OneDrive provide secure data transfer options by encrypting data at rest and during transit, with options for additional layers of security like two-factor authentication.
- Managed File Transfer (MFT): MFT solutions offer centralized, secure, and auditable file transfers by using encryption, access controls, and monitoring to protect data during transit and at rest.
- Remote Desktop Protocol (RDP) over SSL/TLS: Using RDP with SSL/TLS encryption ensures a secure connection between remote clients and servers, allowing for the safe transfer of data between the devices.
- Secure APIs and Web Services: RESTful APIs and web services using HTTPS, OAuth 2.0, and API keys can provide secure data transfer between clients and servers. These security measures ensure that only authorized clients can access and manipulate data.
- Amazon Web Services (AWS) S3 Buckets: AWS S3 is a scalable storage solution that can be used to securely store and transfer data. By default, S3 buckets are private, and data can be transferred securely using SSL encryption. Additional security measures, such as Identity and Access Management (IAM) policies, bucket policies, and encryption options, can be implemented to further protect the data.

Unacceptable Methods of Data Transfer:

- FTP (File Transfer Protocol)
- E-mail
- Third Party file transfer Websites like www.yousendit.com, www.sendbigfiles.com and www.mailbigfile.com

Handling of Data
Only those staff from Vendor assigned to the specific Ipsos project for which the sample is intended may handle the client data provided by Ipsos.

- Vendor must ask Ipsos's permission to transfer Ipsos provided client sample onto any other vendors or sub-Vendors.
- Vendor's sub-Vendors must follow the same procedures for the transferring and handling of Ipsos provided client sample as outlined in this document.

Storage of Data

- Vendor to store Ipsos provided client sample on a server that is physically secured and is only accessed by authorized staff.
- Vendor to store Ipsos provided client sample on a server that is protected behind a firewall and that is properly patched with the latest OS and Security patches.
- Vendor to omit the directory in which Ipsos provided client sample is stored. This is to avoid Ipsos provided client sample from being inadvertently retained on Vendor's backup tapes for an extended period of time.

OR

- Vendor can backup Ipsos provided client sample to backup tapes as long as they are only used for disaster recovery and are not retained. Tape must be overwritten after a set amount of time.

Data destruction process
Vendor must assure that:

- Working storage media will either be wiped, shredded, stored or degaussed;
- Non-working storage media will be shredded, stored degaussed as follows:

Degaussing
For those regions with a degaussing unit, all hard drives and magnetic media such as tapes will be degaussed before disposal.

Hard Disk and Media Storage

- Functioning or non-function hard disks or electronic media such as tapes awaiting destruction by means of shredding, degaussing or wiping must be stored in a secured location with access to the room/safe/filing cabinet only given to those staff who need access to the media.
- A list of who has access to the media will be maintained

- A list inventorying all hard disks and electronic media such as tapes will be maintained and updated as hard disks and electronic media are added/destroyed. The inventory will list the serial number for hard disk and tape labels/names for tapes. The list will also list the status and state of the hard disk.
- This inventory will be reviewed twice a year to check for any lost or stolen hard disks and electronic media.

Media Destruction Standards

- Vendor must consistently demonstrate that they are in control of our information assets (i.e.: hard drive/tapes) up to and including their destruction.
- Confirmation of destruction of our media must be given within next business day of its disposal.
- Hard Drives will be disintegrated to a particle size no greater than ¼ inch or 0.635 cm.
- CD's, DVD's, Backup tapes, audio cassettes, and video cassettes are shredded to ½ inch or 1.27 cm.
- Paper documents will be shredded cross cut on site.

Hard Disk Wipe Standards

- All hard disks ready for destruction or disposal must be wiped using the DBAN utility.
- Wipe Method of US DOD
- 7 passes
- Enable Verification

Data Breach Procedure

A breach of information is any incident that involves the actual or suspected breach of the confidentiality, integrity or availability of an Ipsos information asset. In the case of Vendor, it is referring to the Ipsos provided client sample.

Examples are:

- *Theft or loss of a laptop, PC, USB Key, small computing device or any other computing/storage device that contains any Ipsos provided client sample.*
- *Suspected or otherwise confirmed unauthorized access (hack) into Vendor's network/hosts that holds Ipsos provided client sample.*
- *Successful virus/malware attack on a system that holds Ipsos provided client sample.*

In the event that any Ipsos provided client sample is breached to the public by Vendor, the following incidence response will be carried out by Vendor:

- Vendor shall notify their contact at Ipsos of the breach.
- Vendor will immediately launch an investigation into the data breach.
- Vendor will co-operate with Ipsos in the investigation and will share all relevant system logs and evidence with Ipsos immediately.
- The investigation will examine the root cause analysis in order to determine causes and recommendations for improving Information Security; to prevent future incidences.
- A risk assessment and recommended counter measures will be included in the final report.

Access Management

Vendor must:

- Ensure controls restrict other Vendor customers from accessing Ipsos assets, unless this has been specifically approved in writing by Ipsos
- Use authentication and authorization technologies for service, user and administrator level accounts.
- Not allow Vendor employees or subprocessors direct root access to any systems or access to the administrator user account of any system used in the services provided to Ipsos
- Ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administrator tasks must always be performed using non-administrator user accounts.
- Ensure password policies and standards exist on IT systems that access Ipsos assets
- Ensure systems that access confidential, personal or regulated information require the following password construction requirements at all times:

    i. Minimum length of 8 characters
    ii. Complexity must contain at least three of the following four characters (Number, Uppercase Letter, Lowercase letter, Printable special character)
    iii. When changing or rotating an account password, the reuse of any of the prior 6 passwords is not allowed
    iv. Account password expiration (the requirement to change and existing account password), must occur at - or less than 90 days.
    v. Service accounts must be changed at - or less than 90 days.
    vi. Failed login attempts, when exceeding 3 consecutive attempts, must lock the account.
    vii. Screen saver locks must be enabled to lock access after 30 minutes of user inactivity.

Vendor must ensure systems that access Ipsos assets &/or Ipsos network meet the following additional requirements at all times:

    i. Authentication credentials must be encrypted when stored or transmitted at all times
    ii. Passwords for user-level accounts cannot be shared between multiple individuals
    iii. Vendor must change passwords immediately whenever it is believed that an account may have been compromised.

iv. Passwords must not be communicated via email messages or other forms of electronic communications, other than one-time use passwords.
v. Passwords for individual user accounts must never be given to or shared with
vi. someone other than the account owner
vii. A user's identity must be verified before their password is reset and email or voicemail notification must be sent to notify the user that their password was reset.
viii. First time passwords for new user accounts must be set to unique values that follow the requirements set forth in this policy and must not be generic, easily guessed passwords.
ix. User accounts must be configured to force a change of their password upon first use of a new account or after a password is reset.
x. All manufacturer passwords must be changed from their default values (including when the default value is NULL) and must meet the requirements set forth in this policy. Manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords.
xi. Temporary account passwords, wireless encryption keys, and other default authentication settings.
xii. Password fields must display only masked characters as the user types in their password, where technically feasible.
xiii. Hardcode plain-text passwords must not be used in production environments.
xiv. Production account passwords must not be used in non-production environments.
xv. If a system-level administrator account (e.g. Windows local administrator or UNIX/Linux root) is used to perform privileged management of a device, that password must be changed following completion of that management task.
xvi. If an account has machine-set complex password of 20 characters or more that is never accessed or known by a person, that passwords does not need to be changed during its lifetime, unless the account or its associated system has been suspected of compromise.
xvii. System-level account passwords must be unique on each device.
xviii. All systems must prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels. *Examples include use of sudo or su on UNIX/LINUX systems or "run as" for Microsoft Windows based systems*.

- Vendor must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
- Vendor must ensure procedures exist for provisioning privileged accounts.
- Vendor must periodically review the necessity of privileged access accounts
- If Vendor requires remote access to Ipsos assets, Vendor must always use a Ipsos approved method to remotely connect to any Ipsos asset.

Information Technology Acquisition, Development and Maintenance

Vendor must:

- Ensure infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices
- Ensure industry acceptable application development security standards are followed so that IT systems and applications are tested and secured in every step of the application and system development life cycle.
- Ensure software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

Information Security Incident Management

Vendor must:

- Ensure access and activity audit and logging procedures, including access attempts and privileged access, exist.
- Ensure logging includes all facility, application, server, network device and IDS/IPS logs are centrally managed and maintained for no less than 12 months.
- Ensure security incident response planning and notification procedures exist to monitor, react, notify and investigate any incident related to Ipsos assets.
- Immediately notify Ipsos if Vendor identifies a breach in any controls that impacts the service provided to Ipsos, a Ipsos asset or data related to a Ipsos asset.
- Note: Once Vendor discovers or are notified of a security breach, Vendor must investigate, fix, restore and conduct a root cause analysis.
- Provide Ipsos with results and frequent status update of any investigation related to Ipsos.
- Vendor must permanently inform Ipsos Global Information Security staff on the investigation outcome.

Outsourcing

Where a service is outsourced by Vendor, the process must be managed by the relevant Vendor staff and a contract must be in place that covers all Ipsos information security requirements.

Filing for a policy Exception Request

Information security policy exception requests must be justified by Vendor and approved in writing by the Global Information Security Staff.

ANNEX 2-A

SCC MODULE 2

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers) – Module 2

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 Ipsos entity transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity 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 Annexures 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 Annexures. 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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – 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

Not used

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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annexures as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Annexures to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed 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') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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 for any damages it causes the other Party by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

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

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

CLAUSE 13

Supervision

(a) Where the data exporter is established in an EU Member State: 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) 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 or where neither (a) above nor (c) below apply: 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.

(c) 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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) 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

(a) If the data exporter is established in an EU member state, then these Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

(b) Where clause 13 (b) or (c) applies, 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. The Parties agree that those shall be:

(i) Where clause 13 (a) applies, the courts of the country where the data exporter is established; and

(ii) where clause 13 (b) or (c) applies the course of France.

(b) 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.

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

Data importer(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

B. DESCRIPTION OF TRANSFER

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

C. COMPETENT SUPERVISORY AUTHORITY

(a) *In the case of clause 13 (a), the supervisory authority of the country where the data exporter is located and as can be determined here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.*

(b) *In the case of clause 13 (b) and (c), the* Commission Nationale de l'Informatique et des Libertés - CNIL

3 Place de Fontenoy

TSA 80715 – 75334 Paris, Cedex 07

Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

*Website: **http://www.cnil.fr/** **https://www.cnil.fr/en/contact-cnil***

ANNEX II

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

Technical and Operational Measures (including Security Requirements) as set out in the Agreement

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

ANNEX IV

UK ADDENDUM TO THE SCC

UK Addendum to Standard Contractual Clauses Module 2

BACKGROUND

(A) This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

(B) The Exporter and the Importer (as both are defined below) entered into an agreement to which EU standard contractual clauses and this UK addendum are appended and who together constitute one agreement.

AGREED TERMS

Table 1: Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.

Key contacts	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		Module 3 of the Approved EU SCCs to which this Addendum is appended				
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?
3		no	Authority	Prior	30	-

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: see SCC Module 2, to which this addendum is appended.
Annex 1B: Description of Transfer: as set out in the main body of this agreement, including for any sensitive data transferred
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see SCC Module 2, to which this addendum is appended.
Annex III: List of Sub processors (Modules 2 and 3 only): see SCC Module 2, to which this addendum is appended.

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 x Neither Party

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.

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.

ANNEX 2-B

SCC MODULE 3

Standard Contractual Clauses for Personal Data Transfers from an EU Processor to a Processor Established in a Third Country (Processor-to-Processor Transfers) – Module 3

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 Ipsos entity transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity 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 Annexures 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 Annexures. 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 Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

(iv) Clause 12 –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 Three: Clause 18(a) and (b).

(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

Not used

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 has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 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., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annexures as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Annexures 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.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent

supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed 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') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller, which shall be communicated

via the data exporter. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

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 for any damages it causes the other Party by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

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

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

CLAUSE 13

Supervision

(a) Where the data exporter is established in an EU Member State: 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) 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 or where neither (a) above nor (c) below apply: 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.

(c) 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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) 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). The data exporter shall forward the notification to the controller.

(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, if appropriate in consultation with the controller. 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 controller or 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.

The data exporter shall forward the notification to the controller.

(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.). The data exporter shall forward the information to the controller.

(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. The data exporter shall make the assessment available to the controller.

(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 and the controller 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

If the data exporter is established in an EU member state, then these Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

(a) Where clause 13 (b) or (c) applies, 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

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

(c) The Parties agree that those shall be

Where clause 13 (a) applies, the courts of the country where the data exporter is established; and

where clause 13 (b) or (c) applies the course of France.

(d) 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.

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

Data importer(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

B. DESCRIPTION OF TRANSFER

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

C. COMPETENT SUPERVISORY AUTHORITY

(a) In the case of clause 13 (a), the supervisory authority of the country where the data exporter is located and as can be determined here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

(b) *In the case of clause 13 (b) and (c), the* Commission Nationale de l'Informatique et des Libertés - CNIL

3 Place de Fontenoy

TSA 80715 – 75334 Paris, Cedex 07

Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

Website: ***http://www.cnil.fr/ https://www.cnil.fr/en/contact-cnil***

ANNEX II

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

Technical and Operational Measures (including Security Requirements) as set out in the Agreement

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors or as maybe set out in the main body of the Agreement or in the Purchase Order to which these standard contractual clauses are appended or any amendment thereof:

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

ANNEX IV

UK Addendum to Standard Contractual Clauses Module 3

BACKGROUND

(A) This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

(B) The Exporter and the Importer (as both are defined below) entered into an agreement to which EU standard contractual clauses and this UK addendum are appended and who together constitute one agreement.

AGREED TERMS

Table 1: Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.
Key contacts	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		Module 3 of the Approved EU SCCs to which this Addendum is appended				
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?
3		No	Authority	Prior	30	-

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: see SCC Module 2, to which this addendum is appended.
Annex 1B: Description of Transfer: as set out in the main body of this agreement or in the Purchase Order, including for any sensitive data transferred
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see SCC Module 2, to which this addendum is appended.
Annex III: List of Sub processors (Modules 2 and 3 only): see SCC Module 2, to which this addendum is appended.

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 x Neither Party

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.

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.

ANNEX 2-C

SCC MODULE 2 REVERSE

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers) – Module 2

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 Ipsos entity 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 Annexures 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 Annexures. 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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – 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

Not used

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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annexures as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Annexures to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed 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') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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 for any damages it causes the other Party by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

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

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

CLAUSE 13

Supervision

(a) Where the data exporter is established in an EU Member State: 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) 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 or where neither (a) above nor (c) below apply: 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.

(c) 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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) 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

(a) If the data exporter is established in an EU member state, then these Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

(b) Where clause 13 (b) or (c) applies, 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. The Parties agree that those shall be:

(i) Where clause 13 (a) applies, the courts of the country where the data exporter is established; and

(ii) where clause 13 (b) or (c) applies the course of France.

(b) 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.

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

Data importer(s):

As set out in the main body of the Agreement or the Purchase Order to which these standard contractual clauses are appended.

B. DESCRIPTION OF TRANSFER

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

C. COMPETENT SUPERVISORY AUTHORITY

(a) In the case of clause 13 (a), the supervisory authority of the country where the data exporter is located and as can be determined here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

(b) *In the case of clause 13 (b) and (c), the* Commission Nationale de l'Informatique et des Libertés - CNIL

3 Place de Fontenoy

TSA 80715 – 75334 Paris, Cedex 07

Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

Website: ***http://www.cnil.fr/ https://www.cnil.fr/en/contact-cnil***

ANNEX II

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

Technical and Operational Measures (including Security Requirements) as set out in the Agreement.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

As set out in the main body of the Agreement, the Purchase Order or as recorded in the data exporter's iBuy system, including for any sensitive data transferred.

ANNEX IV

UK Addendum to Standard Contractual Clauses Module 2

BACKGROUND

(A) This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

(B) The Exporter and the Importer (as both are defined below) entered into an agreement to which EU standard contractual clauses and this UK addendum are appended and who together constitute one agreement.

AGREED TERMS

Table 1: Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.

Key contacts	As set out in the main body of the Purchase Order.	As set out in the main body of the Purchase Order.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		Module 3 of the Approved EU SCCs to which this Addendum is appended				
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?
3		no	Authority	General	30	-

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: see SCC Module 2, to which this addendum is appended.
Annex 1B: Description of Transfer: as set out in the main body of this Agreement or in the Purchase Order, including for any sensitive data transferred
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see SCC Module 2, to which this addendum is appended.
Annex III: List of Sub processors (Modules 2 and 3 only): see SCC Module 2, to which this addendum is appended.

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 x Neither Party

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.

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.

ANNEX 3
Insurances policies required by the Vendor

Commercial General Liability (including general liability, property damage, personal and advertising injury, medical expenses, fire damage and employee benefits)

General Aggregate	$2,000,000
Each Occurrence	$1,000,000
Professional Liability	
General Aggregate	$3,000,000
Each Occurrence	$3,000,000
Worker's Compensation	Statutory Limits
Employers Liability (including bodily injury by accident (per accident), bodily injury by disease (policy limit), and bodily injury by disease (each employee)	$1,000,000
Cyber Liability	
General Aggregate	$5,000,000
Each Occurrence	$5,000,000

The amounts stated above are considered to be minimum amounts and shall in no event constitute a limitation of the Vendor's liability under the Agreement. The Vendor and its subcontractors shall bear the cost of any deductible amounts applied to them by their insurers.

ANNEX 4
ESG – CLIMATE ACTION

Definitions. For the purposes of this document:

(a) "ESG" means all the aspects of ESG including environmental, social and governance factors considered by companies, investors, public sector and other organizations in a wide range of decision-making processes and situations including strategy, purpose financing, company reporting and supply chain management. In the context of this Agreement, ESG also refers to environmentally sustainable objectives including climate change mitigation; climate change adaptation; the sustainable use and protection of water and marine resources; the transition to a circular economy, waste prevention and recycling; pollution prevention and control; and the protection of healthy ecosystems and biodiversity;

(b) "GHG Reporting Standards" means the standards for the measurement, reporting and management of greenhouse gases published by the Greenhouse Gas Protocol;

(c) "Greenhouse Gas Protocol" means the Greenhouse Case Protocol promulgated by the World Resources Institute (WRI) and the World Business Council for Sustainable Development (WBCSD); and

(d) "Product Carbon Footprint" means the total Greenhouse Gas Emissions over the whole life of any Services and supplied products, from the extraction of raw materials and manufacturing through to its use and final re-use, recycling or disposal, including Scope 1, Scope 2, and Scope 3 Emissions (as defined in the Greenhouse Gas Protocol), as described in the Greenhouse Gas Protocol.

Vendor shall: (i) use reasonable efforts to reduce carbon emissions and its impact on climate change. Membership of initiatives like the Science-Based Targets Initiative (SBTi) and other commitments to reaching Net Zero by 2050 at the latest are strongly encouraged by Ipsos, although they are not mandatory; (ii) use reasonable efforts to meet the principles of a circular economy in its operations and products, where possible; (iii) use its best efforts to minimize any waste materials and to turn waste materials into diverted waste, where possible.

ESG Report: Vendor represents and warrants that it will maintain complete and accurate records of all greenhouse gas emissions and other related ESG metrics associated with the performance of the Services. Vendor shall provide this information to Ipsos in an annual ESG Report which shall include (i) a summary of the commitments from the Provider on sustainability (Net Zero or carbon neutrality plans etc.) and a list of the policies in place in that area (e.g. switch to renewable energies, recycling of electronic equipment, policies for limiting water consumption, especially for air conditioning systems/cooling systems etc.), (ii) a summary of Vendor's actions promoting diverse and inclusive work environments, (iii) details on ESG metrics used by Vendor and (iv) a summary of the industry best practices on managing and reducing GHG Emissions applied by the Supplier in the previous year, and how these have been applied.

Vendor shall provide the ESG Report within forty (40) business days after the end of each calendar year, and more frequently as Ipsos may reasonably request. Vendor shall commission an independent third party, at Vendor's sole cost and expense, to independently verify and confirm all information contained in the ESG Report and provide Ipsos with a certification from such third party that the information within the ESG Report is true and accurate in all material respects. At Ipsos' option, the parties shall meet quarterly to review Vendor's sustainability performance, including Vendor's greenhouse gas and "green" objectives, industry best practices, the emergence of new and evolving relevant technologies and processes, an overview of Vendor's ESG metrics, and the Vendor's improvement initiatives. The ESG Report shall be provided in both pdf and csv formats sent by email to the Ipsos ESG Director (Supplier Compliance&ESG@ipsos.com), as well as to Vendor's regular Ipsos contact, who will both acknowledge receipt of the documents. Vendor shall also provide at the effective date of the Purchaser Order to Ipsos a declaration of certification (ISO, etc…) and Vendor's ESG policy if available.

ANNEX 5
HEALTHCARE COMPLIANCE

1.1 General: Where the Services relate to healthcare and/or pharmaceutical market research, the Vendor represents, warrants, and covenants to Ipsos ("**Ipsos or the "Client**") that it shall:

(a) adhere to all applicable market research and pharmaceutical industry codes of conduct, guidelines and best practices including, but not limited to EPHMRA's Code of Conduct and Adverse Event Reporting Guidelines, BHBIA's Legal and Ethical Guidelines and Guidance on Reporting Adverse Events, as they apply to the Services being provided under this Agreement;

(b) ensure that each person assigned to perform the Services has the appropriate level of expertise, training and where applicable certificates necessary to perform such Services; and,

(c) provide copies of training certificates to Client on request.

1.2 Adverse Event Reporting:

(a) An "**Adverse Event"** or **"AE"** is any untoward medical occurrence in any patient, clinical investigation subject or other individual who is administered a drug or any other pharmaceutical or medicinal product, whether or not such occurrence has a causal relationship with, or is related to such drug or product, including, but not limited to, any unfavorable or unintended sign (including, for example, any abnormal laboratory finding), symptom, or disease temporally associated with the use of such a drug or product.

In the context of the Agreement, AE is to be considered an umbrella term that encompasses multiple issues such as adverse events, adverse reactions, product complaints, and special reporting situations.

By way of example and without limitation, the following events are considered Adverse Events, each case of which must be reported by Vendor in line with the obligations set out in clause 1.2(b):

- Side effects (with or without causal link)
- Lack of efficacy
- Disease progression or aggravation
- Abnormal test findings
- Unexpected therapeutic reaction / unexpected benefit
- Drug exposure during pregnancy (via the mother or father, with or without outcome)
- Drug use during lactation or breastfeeding
- Overdose (intentional or unintentional)
- Abuse
- Misuse
- Withdrawal or rebound symptoms
- Medication error (dispensing errors / maladministration)
- Drug-drug, drug-food, drug-beverage interactions
- Product quality or technical complaint (with or without AE)
- Device related incidents
- Suspected counterfeit medicine
- Off-label use
- Occupational exposure / accidental exposure
- Compassionate use (expanded access)
- Suspected transmission of an infectious agent
- Death / hospitalization

For a more detailed list of Adverse Events and criteria for reporting, the Vendor shall refer to the guidelines/trainings document issued by the Client for each project as provided by Client, where applicable.

(b) While providing any Services relating to healthcare and/or pharmaceutical market research, the Vendor warrants that it will report any AE to Client or, if required by Client, directly to the end-user client's ("**End Client**") Drug Safety department within one business day or any other timeframe as required by the End Client. If Client wishes for Vendor to notify their End Client directly, Client will provide Vendor with the contact information. Vendor must always keep Client in copy for any such communication. All individual Adverse Events will be reported using a specific AE reporting form of the pharmaceutical company or as provided by Client. To ensure compliance, the Vendor shall:

i. prior to the start of any project, liaise with Client to agree on the details of the Adverse Event reporting procedure for each such project;
ii. ensure that these obligations are communicated to, and complied with by, its personnel, including employees and subcontractors;
iii. train all Vendor personnel, including employees and subcontractors, assigned to Client projects on Adverse Event reporting prior to the beginning of any applicable project, such training materials and/or relevant information will be provided to the Vendor by Client;
iv. document all Adverse Event training activities including the topic of the training, trainer name (if applicable), date of training and the name and signature for each trainee;
v. file all original copies of such training documentation at the Vendor site, and provide copies to Client prior to the beginning of any applicable project;
vi. ensure Vendor has the rights to share training records with Client for all Vendor personnel and subcontractors, prior to providing such documentation to Client;
vii. for projects conducted with respondents within the United Kingdom, Vendor shall also adhere to the BHBIA/ABPI Adverse Event Guidelines for Market Research;
viii. prior to the interview or questionnaire administration, inform all research participants that any Adverse Event identified during the course of the study will be reported to Client or, if required by Client, directly to the End Client's Drug Safety department within the agreed timeframe and, subject to research participant's informed consent where legally permitted, that Client may contact them for additional information regarding the Adverse Event;
ix. with the exception of research participants in any country where seeking consent to waive anonymity is prohibited, include a suitably worded consent question seeking research participant's consent to the disclosure of their name and contact details with any Adverse Event report made to Client or, if required by Client, directly to the End Client's Drug Safety department;
x. in those countries where seeking consent to waive anonymity is prohibited, in the event of an Adverse Event being identified, seek research participant consent to be re-contacted either by Vendor or Client on behalf of the End Client;
xi. inform all research participants that regardless of any consent given in relation to reporting Adverse Events, all responses not related to any Adverse Events will be treated in the strictest of confidence in accordance with standard Market Research Codes of Conduct. Client will provide the Vendor with the disclaimer paragraph to be used in every project for this purpose.
xii. monitor all respondent responses in order to identify potential Adverse Events, special situations and product complaints;
xiii. complete the reporting form with all available and relevant information;
xiv. assign an ID for each reportable AE (as standard, for Quant projects use Respondent ID and for Qualitative projects use interview reference number or respondent ID as used to label each participant);
xv. validate content of completed reporting form prior to submission for
a) completeness of information, and
b) integrity of information;
xvi. relay all Adverse Event and other relevant information to Client or, if required by Client, directly to the End Client's Drug Safety department within one business day or any other timeframe as required by the Client of an Adverse Event being identified or of an Adverse Event being mentioned by a respondent;
xvii. where applicable, ensure to obtain confirmation of receipt by Client or by End Client within one (1) business day; if Vendor does not receive such confirmation, Vendor must contact designated point of contact to determine if the report was received. Vendor will maintain a record of the confirmation;
xviii. cooperate with Client and the End Client in case any follow ups with research participants are necessary;
xix. cooperate with Client in implementing any additional or amended Adverse Event reporting requirements required to comply with the Client's contractual requirements set out in the Agreement or Work Order or otherwise agreed to in writing.

(c) After the completion of each project, or at different agreed intervals, Vendor must complete a summary of all Adverse Events, special situations and product complaints that were reported. A reconciliation form will be provided by Client and must be completed regardless of the number of Adverse Events identified and reported during the project, even if the number is zero. Such form will be submitted to Client' project manager and/or to the End Client if so required.

(d) If any personal data related to reportable Adverse Events, special situations and product complaints is being exchanged by e-mail, the information must be attached to the e-mail in form of password protected files and encrypted in transit using AES 256 bit or stronger encryption.

(e) In the event the Vendor engages subcontractors to perform services related to Client projects, the Vendor shall:

i. obtain Client authorization prior to engaging any subcontractor;
ii. require fulfilment by the subcontractor of these Adverse Event reporting requirements on substantially the same terms as those outlined in this Agreement.

1.3 Storage of AEs

Vendor must retain the following information for an unlimited period or for such period as may be agreed between the parties:

i. all relevant source data;
ii. AE forms completed for every AE on every project;
iii. evidence of sending AE forms to the Client's Drug Safety department;
iv. confirmation of receipt from the End Client's Drug Safety department.

At completion of Services, Vendor shall transfer all relevant project material (including but not limited to original source data, any pharmacovigilance related material and correspondence such as those stated above in article 1.2) to Client, for Client to retain in accordance with their own requirements. The Vendor is responsible to ensure all project related material is safely received by Client.

Before any data is destroyed, Vendor must obtain authorization from Client. Client might request at that point for data to be transferred to Client for confidential longer-term storage.

1.4 Audit

Without prejudice of any other audit right provided to Ipsos herein, for the term of this Agreement and three (3) years following expiration or termination hereof, Client, its designated third-party auditor or End Client, shall have the right to audit with reasonable prior notice the supplier´s processes, procedures and training, including records, data, documentation with respect to AEs in relation to the services provided to Client.

Vendor commits to correcting issues from audit observations within the mutually agreed timelines and promptly communicating the actions to Client.

1.5 Incentive Payments for Healthcare Projects

(a) Any proposed incentive payment provided to a market research participant must be based on fair market value (FMV), in local currency and clearly identified in service letter/proposal.

Vendor must pay incentives to participants in accordance with all respective regulations in the relevant country and all Codes of Conducts applicable.

In addition, Vendor and where relevant their subcontractors must comply with the following considerations when paying incentives to participants:

i. As standard, the only payment solutions accepted by Client are by bank transfer, checks, or vouchers;
ii. Other types of incentive payments must be approved by Client and its End Clients in writing;
iii. In those cases where an exception is granted within the service letter/proposal Vendor must keep in its books all proofs of payments made to participants, such as receipt signed by participant in case of physical exchange of a voucher, and shall make them available to Client on demand;
iv. In no event will Vendor provide an additional or higher incentive to any participant than is indicated in the service letter/proposal, unless such increase has been discussed with and approved by Client in writing;
v. Vendor recognizes that payments to government employees and HCPs within certain countries and states are restricted and will abide by such restrictions.

(b) **Transparency Reporting**: Vendor shall comply with all applicable national laws, regulations, and industry guidelines in regard to transparency of incentive payments to market research participants (e.g., US Sunshine Act, Loi Bertrand and Loi Anti-Cadeaux in France, etc.).

If applicable, Vendor represents that it has procedures in place to track, document, and report payment of incentives to local authorities on behalf of Client and its End Clients.
Upon demand, Vendor shall be able to produce evidence of their compliance with applicable national laws, regulations, and industry guidelines.

On a project-by-project basis, Client might be required to report incentive payments (including any expenses paid) to its clients; in such cases, Client and Vendor will discuss and agree prior to start of the Services how to comply with such transparency reporting requirements. Vendor warrants to provide Client and its End Clients with the necessary information to comply with such requirements.

ANNEX 6
SPECIFIC PURCHASING TERMS FOR IT SERVICES

THESE SPECIFIC PURCHASING TERMS FOR IT SERVICES SHALL APPLY IN ADDITION TO THE IPSOS PURCHASING TERMS IF VENDOR PROVIDES TO IPSOS SOFTWARE LICENSES AND ANY RELATED IT SERVICES SUCH AS PROFESSIONAL SERVICES, MAINTENANCE, SUPPORT SERVICES OR HOSTING SERVICESTO IPSOS ("IT SERVICES")

"User(s)": means, as applicable, any authorized person within Ipsos and its Affiliates worldwide, its respective employees, agents, subcontractors, contractors and Ipsos' end clients, a Panel Member or a Community Member (if any) who have been supplied license keys or other permitted access details by Ipsos. **"Panel Members/Community Member(s)"** means a pre-recruited individual who has agreed to take part in market research activities and be continuously surveyed.

1. SOFTWARE LICENSE AND PROVISION OF IT SERVICES

(a) Subject to the **Ipsos Purchasing Terms**, Vendor grants to Ipsos and/or its Affiliates a worldwide, non-exclusive, non-transferable, non-sub licensable usage license to (a) access, deploy, install and use the software as identified in the Purchase Order (including any updates, improvements or enhancements made by the Vendor) ("**Software**") through and for each User (as specifically defined in the Purchase Order) and also for or on behalf of Ipsos's clients in the territory identified in the Purchase Order, in accordance with the Software's documentation, and (b) access and use the Software for Ipsos' own internal business purposes ("**Software License Grant").** The terms of the Software License Grant shall be identified in the Purchase Order. Upon the effective date of the Purchase Order, Vendor shall issue to Ipsos and shall provide an Ipsos administrator with a user password to download and install the Software and the documentation. Ipsos and its Users are responsible for maintaining the confidentiality of all passwords at all times. Ipsos shall promptly inform Vendor if passwords are being compromised.

(b) Ipsos shall not do any of the following: (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code for, or underlying algorithms of the Software; (ii) modify, translate, or create derivative works based on the functionality contained in the Software (except for reversibility purposes; (iii) rent, lease, distribute, sell, assign, or otherwise transfer its rights to use the Software; or (iv) use the Software on a timesharing or service bureau basis or otherwise for the benefit of a third party other than the Ipsos's end clients and the authorized Users of the Software License Grant as set forth in this Section.

(c) During the Term and at no additional charge to Ipsos, Vendor shall provide Ipsos access to and maintain online documentation, accessible via the Internet, documenting application features and functionality, including but not limited to existing APIs. The Vendor shall, from time to time, promptly deliver a copy of any revised, updated or supplemental documentation to Ipsos, at no additional costs to Ipsos. Ipsos may reproduce any such documentation as reasonably necessary to support internal use of the Software.

(d) Vendor shall maintain a regular Software update and development lifecycle in order to allow Ipsos to use the latest up-to-date version of the Software and hardware technology possible. Vendor warrants that any change to the specifications of the Software will not diminish the features and functionalities contained in the Software. No changes to the Software may be implemented without Ipsos' prior written approval (which shall not be unreasonably withheld) except as may be necessary on a temporary basis to maintain continuity of any maintenance of IT Services.

(e) Vendor will maintain the Software at a reputable third-party Internet service provider (either directly or through Ipsos e.g. via Amazon Web Services) that has a current 3rd party audit report for Information Security controls such as SSAE 18 SOC 2, ISO 27001, ISO 020252. In addition, the hosting facility will guarantee the privacy, security, integrity or authenticity of any information so transmitted over or stored in any system connected to the Internet or that any such security precautions will be industry standard.

(f) If Vendor hosts Ipsos data or Personal Data, Vendor shall host such data in compliance with the provisions contained in the agreed SLA (if any) during the Term. Vendor's data servers shall be located in the EU (European Union).

(g) If the Software and/or any Ipsos data or Personal Data are being hosted by the Vendor, Ipsos has the right to request Vendor , at any time or in case of termination of a Purchase Order, from Vendor's servers to delete or erase any such data (including any database or copy of the database) in a format compatible with "Microsoft SQL Server" or in any other format as requested by Ipsos as well as any back-ups ("Disposal") according to Ipsos' specific instructions and at no cost for Ipsos. Vendor shall not contract out such Disposal or involved any third parties in this process without the prior written consent of Ipsos. After 30 days, Vendor will certify such deletion or erasure in writing to Ipsos. Deletion or erasure refers to the destruction of such data so that no copy of such data remains or can be accessed or restored in any way.

(h) Ipsos shall be entitled to the benefits of any standard Service Level Agreement(s) **"(SLA(s")** offered by the Vendor. Vendor hereby commits to provide such SLA(s) to Ipsos upon request. Ipsos reserves the right to request penalties from the Vendor for any breach of the service levels agreed in an SLA. Notwithstanding the foregoing, the Vendor shall ensure that the IT Services are available to Ipsos at least 99% of the time during any calendar month, failing which Ipsos may impose penalties as per the terms agreed upon. Vendor shall from time-to-time issue to Ipsos new releases, containing error corrections and updates. Vendor will provide Ipsos with one copy of each release for each copy of the Software without additional charge.

The application of any penalties or service credits does not mean that Ipsos waives the requirement for Vendor to comply with any key dates or milestone or a Service Level. The penalties/service credits are due without prejudice of any right to possible compensation or claim by Ipsos due to damage suffered as a result of the non-compliance with any key dates or milestone or any service levels by Vendor. Ipsos is entitled to receive a refund of the fees paid by Ipsos to Vendor or to set off any compensation against any next fees or amounts to be paid by Ipsos to Vendor or to ask Vendor to issue credit notes for the same amount. Ipsos's decision not to apply this clause shall not be construed as a waiver of the right to impose penalties. Under no circumstances should the Vendor be permitted to withhold support, even if there is a dispute between the parties.

(i) At Ipsos' request, Vendor will train Ipsos' personnel, in presence or remotely based on the agreement of the parties on the use and operation of the Software and the Work Product in order to ensure Ipsos may use the Software, the IT Services and the associated documentation or on behalf of Ipsos' end clients, and to provide ongoing instruction and training to Ipsos' personnel on a periodic basis.

2. TEMPORARY UNAVAILABILITY OF THE SOFTWARE

(a) Vendor will be able to suspend the access to the Software, subject to ten (10) business days, prior notification of Ipsos, and subject to providing to Ipsos relevant justification for the suspension in the following case and on the condition that none of the below has been caused by Vendor or as a result of its gross negligence or willful misconduct:

- the suspension is required to perform scheduled maintenance or scheduled updates,
- the suspension is required by any applicable laws, regulations or by a Court decision.

(b) Vendor shall not be liable for any justified interruption or suspension of the Software if and to the extent such interruption or suspension of the Software is caused by the cases above. Vendor will provide best efforts to restart the Software promptly as possible and to mitigate the impact of the suspension. Vendor will not charge Ipsos a fee for restarting Software.

(c) In the event of an external attack (such as a DDoS attack), Vendor will implement and employ various mitigations and tactics to reduce the attack as per the Vendor's mitigation plan that will be part of the SLA.

3. DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

Vendor represents and warrants to Ipsos that it has and will maintain a disaster recovery and business continuation plan **("BCP")** for multiple scenarios and expected disaster profiles that enable Vendor to continue to provide the Services in accordance with the Ipsos Purchasing Terms, these Purchasing Terms for IT Services or any Purchase Order. The BCP will be tested, revised and updated yearly or with new system/infrastructure changes to ensure continued operability. A documented test of the BCP by means of a desk exercise or scenario role play will be done yearly. Vendor shall provide a copy of such BCP to Ipsos for approval, within 30 days from (i) the Term and (ii) each revision or update of such BCP. Vendor will implement and activate the BCP upon the occurrence of any event materially affecting Ipsos' timely receipt of the IT Services and/or the Work Product and shall restore the same level of service of the Vendor's applications to Ipsos. Vendor will work with Ipsos to agree on BCP objectives.

4. AUDIT

(a) In addition to the provisions contained in the Ipsos Purchasing Terms, Vendor and Ipsos (or Ipsos end client if it is the case) shall meet to review each audit report (or extract) promptly and to mutually agree upon an appropriate and effective manner in which to respond to any deficiencies identified and modifications suggested by the audit report. If any audit report indicates that Vendor or its agents or its authorized sub-processor's/subcontractors are not in compliance with any applicable law, audit, or other requirement applicable to Vendor pursuant to the Terms, Vendor shall take, and shall cause its agents to take, prompt actions to comply with such requirement and Vendor shall refund any overcharge. Vendor shall bear any cost and expense to implement any such response that is (i) required by any law or audit requirement relating to Vendor's business or (ii) necessary due to Vendor's non-compliance with any law, audit, or other requirement applicable to Vendor pursuant to the Agreement.

(b) If, as a result of such audit, Ipsos or its designated third party auditor reasonably determines that Vendor has overcharged Ipsos under a Purchase Order, Ipsos shall notify Vendor of the amount of overcharge and Vendor shall promptly pay to Ipsos the amount of the overcharge, plus (i) the reasonable costs, expenses Ipsos incurred in conducting the audit, and (ii) interest on such overcharged amount at the rate of 1,5% per month or the highest interest charge allowed under applicable law, whichever is the less.

(c) Independently of the other audits and inspections, Ipsos shall have the right to receive a copy of the operational journals, incident reports, reports for interventions concerning the execution of the IT Services. Such copies shall be made available without any formality or additional costs.

(d) Vendor shall fill out an Ipsos Information Security Assessment form before engagement begins. Vendor can submit a SSAE 18 SOC 2 or ISO 27001 audit in lieu of filling out the report. The form must be filled out every two (2) years.

(e) If Vendor is hosting Ipsos information, a vulnerability scan of the servers/infrastructure that will be hosting Ipsos information is required. Vendor has a choice of submitting an auditor's scan report in lieu of Ipsos performing the scan. The scan must be completed before the infrastructure or applications become live and in production.

(f) If Vendor has created a web application for Ipsos, an application vulnerability scan of the application will be done (to test for application vulnerabilities such as Cross Site Scripting, SQL Injection etc.). The time for the scan must be before the application has been released into production. The Vendor has the choice of submitting an auditor's scan report in lieu of Ipsos performing the scan. An application vulnerability scan must be conducted yearly during the course of the engagement and the results provided to Ipsos upon its request.

5. REVERSIBILITY

Vendor must take all measures and actions to enable Ipsos, when a Purchase Order or any IT Services terminates for any reason whatsoever, to allow Ipsos or a third-party provider appointed by Ipsos to take over all or part of the Services following termination or expiration of a Purchase Order or an IT Service for any reason whatsoever; ("**Reversibilit**y") with Vendor's cooperation and assistance. If Ipsos data have been stored on mutualized storage and safeguard resources, it must be possible to extract them without difficulty and within lead times compatible with the transfer operations thus causing a very limited stopping period in the operation of Ipsos' applications with the reasonable technical assistance of Vendor necessary for exercising the Reversibility plan. The Reversibility phase starts as from (i) the notification in case of early termination or (ii) upon termination of the Purchase Order or the relevant IT Service. The Reversibility Phase will be for a duration of 8 (eight) months unless otherwise agreed by the parties at the beginning of the Reversibility phase or extended by mutual agreement.

During the Reversibility phase, all the IT Services are maintained to the levels set out in the SLA (if any). The Reversibility plan shall be prepared in advance by Vendor and shall be delivered to Ipsos within 3 (three) months following the effective date of the Purchase Order. The Reversibility plan shall be subject to approval by Ipsos. The parties shall negotiate in advance in good faith the Reversibility fees which will be based on fair and competitive market prices. The Reversibility fees are not charged by Vendor to Ipsos in case of termination of a Purchase Order or an IT Service by Ipsos for a cause not attributed to Ipsos.