KANTAR

TERMS AND CONDITIONS
(PURCHASE OF SERVICES)

1. **DEFINITIONS**

1.1. In this Agreement, the following words shall have the following meanings:

1.1.1. **"Affiliate"** shall mean any entity which, directly or indirectly through one or more intermediaries, Controls, or is Controlled by, or is under common Control and in the case of Customer is trading as Kantar from time to time, but excluding Europanel.

1.1.2. "**Agreement**" means together the Purchase Order and these Terms

1.1.3. **"Confidential Information"** means any information relating to the Customer's and/or any member of the Kantar Group's directors, officers and employees, budgets, prices, order book, methodologies, questionnaires accounts, finances, parent and subsidiary companies, Customer Data and its customers and clients.

1.1.4. "**Control**" shall mean (a) possession, direct or indirect, of the power to direct the management or policies of such entity, whether through ownership of voting securities, by contract relating to voting rights, or otherwise or (b) ownership, direct or indirect, of more than fifty percent (50%) of the outstanding voting securities or other ownership interest of such entity.

1.1.5. **"Customer"** means the Kantar Affiliate named on the Purchase Order.

1.1.6. "**Customer Data**" means any data (including any Personal Data relating to staff, customers/clients or suppliers of the Customer or its clients), documents, text, drawings, diagrams, specifications, images (together with any database made up of these) supplied or made available to the Supplier by or on behalf of the Customer or its clients, or which the Supplier is required to generate, process, store or transmit pursuant to this Agreement.

1.1.7. **"Data Protection Legislation"** means the GDPR and the European Privacy and Electronic Communications Directive (as amended from time to time) and any legislation implementing those Directives in any country.

1.1.8. **"Deliverables"** means all goods, items, equipment and materials to be supplied as part of the Services.

1.1.9. **"Fees"** means the total sum to be paid by the Customer as stated on the Purchase Order.

1.1.10. **"GDPR"** means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.1.11. **"Intellectual Property Rights"** means all patents, rights to inventions, copyright and related rights, moral rights, database rights, semiconductor topography rights, utility models, rights in designs, trade marks, service marks, trade names, domain names, rights in goodwill, rights in undisclosed or confidential information, and other similar or equivalent rights or forms of

protection as may now or in the future exist anywhere in the world.

1.1.12. **“Personal Data”** has the meaning given in Schedule 3.

1.1.13. **"Purchase Order"** means the purchase order attached to these Terms and Conditions or any other form of written communication which references the Purchase Order number and to which these Terms and Conditions shall apply.

1.1.14. **"Services"** means the services specified in the Purchase Order or the reference of the Purchase Order number specifying the services in any other form of written communication.

1.1.15. **"Supplier"** means the entity identified in the Purchase Order.

1.1.16. **"Supplier Personnel"** means all personnel required to perform the Services.

1.1.17. **"Supplier Policies"** means all policies or codes of conduct applicable to the suppliers of The Kantar Group Limited. and its direct or indirect subsidiaries, as notified by the Customer to the Supplier from time to time or as made available on any extranet operated by the Customer for its suppliers from time to time (which will be made available upon request), including, but not limited to, the Kantar Code of Business Conduct attached hereto as Schedule 1 and any applicable Kantar anti-bribery policies.

2. **THE SERVICES**

2.1. These Terms and Conditions shall apply to the Services.

2.2. The Purchase Order shall be deemed accepted upon commencement of the Services. The Supplier shall provide the Services from the date specified on the Purchase Order. The Supplier shall provide the Services to the Customer in accordance with the Customer’s requests from time to time, the Supplier Policies, best industry practice and the terms of this Agreement. Time for the performance of the Services shall be of the essence.

2.3. The Supplier warrants that each of the Supplier Personnel:

2.3.1. shall comply with the Supplier Policies as updated from time to time;

2.3.2. are suitably qualified and trained in order to provide the Services;

2.3.3. have been appropriately screened in accordance with any specific instructions issued by the Customer, and do not have any criminal convictions; and

2.3.4. are entitled to work in the territory in which the Services are being provided.

2.4. Supplier warrants, undertakes and represents on an ongoing basis that:

2.4.1. it has full capacity and authority to enter into and perform its obligations under this Agreement;

2.4.2. it is in compliance with all applicable laws, regulations and codes of practice;

2.4.3. it will not do any act or make any omission in relation to the performance of its obligations under this Agreement which does or may adversely materially affect the reputation of the Customer or its client; and

2.4.4. the Deliverables are complete, accurate, non-infringing and

compliant in all respects with this Agreement.

3. **FEES**

3.1. The Supplier shall only be entitled to invoice the Customer upon completion of the Services to the Customer's reasonable satisfaction. The Customer shall pay the Fees for the Services on the Customer's next payment run following a date which is sixty (60) days after the end of the month in which a valid invoice specifying the correct PO number is received. Where the Services are procured from the Supplier by the Customer acting for the benefit of a client, the Customer shall not be obliged to make payment to the Supplier until it has received payment from the client. The Fees are exclusive of sales or similar taxes. The Customer shall be entitled to make deductions or withholdings from the Fees where required by law.

3.2. The Supplier may charge interest on any undisputed overdue sum at the rate of 2% above the Bank of England base rate per annum.

4. **TERMINATION**

4.1. The Customer may terminate this Agreement, in whole or (with a proportionate reduction in the Fee) in part, at any time:

4.1.1. for convenience on thirty (30) days' written notice to the Supplier; or

4.1.2. immediately if the Supplier is in material breach of this Agreement which is not remedied within 14 days of the Supplier being given notice to do so by the Customer; or

4.1.3. immediately if an order is made or a resolution is passed for the winding up of the Supplier, or the Supplier has a receiver or administrator appointed of any part of its assets, or circumstances arise which entitle the court or a creditor to appoint a receiver or manager or a court to make a winding up or administration order, or makes an arrangement with creditors or if the Supplier is unable to pay its debts as and when they fall due.

4.2. Upon expiry or termination of this Agreement or of any part of the Services, the Supplier will deliver all Confidential Information to the Customer and liaise with the Customer and/or third party to ensure a satisfactory handover.

4.3. Expiry or termination of this Agreement shall be without prejudice to any rights accrued up to the date of termination or any provisions which expressly or impliedly survive termination.

5. **AUDIT**

5.1. The Supplier shall keep and maintain at its principal place of business true and accurate written books and records in connection with the Services (including but not limited to timesheets, claims records, invoices, expenses, costs, credit notes) in accordance with generally accepted accounting and document retention principles during this Agreement and for a period of 6 years thereafter and permit the Customer and/or its client or the Customer's authorised representative to inspect such records upon reasonable written notice for the purposes of assessing compliance with this Agreement (including, without limitation, the restrictions set out in Clause 10).

5.2. If, as a result of an audit, the Customer discovers any overpayment in relation to the Services or any other non-compliance with the terms of this Agreement, the Supplier shall promptly rectify such non-compliance at its own cost and refund to the Customer the full amount of any overpayment and the costs of the relevant audit.

6. **LIABILITY AND INDEMNITY**

6.1. Nothing in this Agreement shall exclude or limit either party's liability in respect of any claims:

6.1.1. for death or personal injury caused by the negligence of such party; or

6.1.2. resulting from any fraud including fraudulent misrepresentation made by such party; or

6.1.3. for which liability may not otherwise lawfully be limited or excluded; or

6.1.4. for any indemnity provided by the Supplier to the Customer under this Agreement; or

6.1.5. for any breach by the Supplier of Clauses 8 to 10 inclusive or 12.1; or

6.1.6. for any deliberate or wilful default by the Supplier.

6.2. Subject to Clause 6.1, the Customer shall not be liable for any indirect, special or consequential losses or any loss of profits (whether direct or indirect), loss of goodwill, loss of business, loss of revenue or loss of anticipated savings.

6.3. The Supplier shall indemnify the Customer against all losses, costs, liabilities, damages, expenses, claims and proceedings incurred and/or suffered by the Customer arising out of or in connection with:

6.3.1. any breach of this Agreement; or

6.3.2. any loss of or damage to property of the Customer during the provision of the Services; or

6.3.3. any negligent act or omission by the Supplier, the Supplier Personnel and/or sub-contractors or their employees in connection with this Agreement; or

6.3.4. any claim that the use of the Deliverables and/or Services infringes the Intellectual Property Rights of any third party.

6.4. Subject to Clauses 6.1 and 6.2, the Customer's total aggregate liability arising from or related to this Agreement (whether in contract, tort including negligence or otherwise) shall not exceed an amount equal to the Fees paid or payable to the Supplier by the Customer under this Agreement in the twelve (12) months preceding the event that triggered such liability.

6.5. Subject to Clauses 6.1 and 6.2, the Supplier's total aggregate liability arising from or related to this Agreement (whether in contract, tort including negligence or otherwise) shall not exceed £10,000,000 (ten million pounds sterling) per claim.

7. INSURANCE

7.1. The Supplier shall take out and maintain with a reputable third party insurer insurance to cover the Supplier's obligations and liabilities under this Agreement and:

7.1.1. in respect of its public liability, to a minimum value of £1,000,000 for any one event and unlimited in the relevant insurance period;

7.1.2. in respect of its employer's liability, to a minimum value of £5,000,000 for any one event and unlimited in the relevant insurance period; and

7.1.3. in respect of its professional indemnity liability, to a minimum value of £1,000,000 for any one event and unlimited in the relevant insurance period.

7.2. Each such policy shall name the Customer as additional insured and shall contain an indemnity to principals clause. Each such policy shall not call into contribution and shall not be in excess to any other insurance available to the Customer. The Customer shall not be liable in respect of any deductibles payable and such deductibles shall be no less than £50,000.

7.3. The Supplier shall take out such additional insurance cover as the Customer shall reasonably require from time to time.

8. **DATA PROTECTION**

8.1. If the provision of the Services requires the Processing of Personal Data by the Supplier on behalf of the Customer, the Supplier will:

8.1.1. comply with the Data Protection Legislation;

8.1.2. act only on the instructions of the Customer as data controller;

8.1.3. comply with Schedule 2 (Information Security Addendum);

8.1.4. comply with Schedule 3 (Data Protection).

8.2. The Supplier shall indemnify the Customer against all losses, liabilities, claims, expenses, damages and costs suffered or incurred by the Customer as a result of the Supplier's failure to abide by the Data Protection Legislation, this Clause 8 and the provisions of Schedule 3.

8.3. The Supplier shall comply with the specific terms required by GDPR relating to any Services that require the processing of Personal Data as set out in Schedule 3.

8.4. The Supplier warrants that it shall have in place measures which incorporate the ISO/IEC 27001 information security standard or any such equivalent standard that replaces it from time to time.

9. **INTELLECTUAL PROPERTY RIGHTS**

9.1. Subject to Clause 9.3, the Customer shall own the Intellectual Property Rights in the Deliverables and the Supplier hereby irrevocably and unconditionally assigns with full title guarantee to the Customer all and any Intellectual Property Rights, upon creation of the same, in the Deliverables. The Supplier shall, and shall procure that the Supplier Personnel waive in favour of the Customer absolutely and irrevocably their moral rights (if any) in relation to such Deliverables.

9.2. Nothing in this Agreement is intended to affect the Supplier's ownership of materials used or developed by it independently of the Services or the Supplier's generic methodologies, tools, technology or processes which are used by it (but not developed by it) in the performance of the Services (together the "**Supplier's Pre-Existing Materials**"). If the Supplier's Pre-Existing Materials (or part thereof) are incorporated in the Deliverables, or required to use or exploit the Services, the Supplier hereby grants to the Customer a perpetual, worldwide, irrevocable, non-exclusive, royalty-free licence to use the Supplier's Pre-Existing Materials to enable the Customer to obtain the full benefit of the Services.

9.3. The Supplier warrants and represents that it has the right to assign or license all Intellectual Property Rights granted or assigned pursuant to this Agreement and that the grant and terms of its respective assignment or licence shall not infringe the Intellectual Property Rights of any third party.

9.4. The Supplier shall not acquire any right, title or interest in or to any Intellectual Property Rights owned by or licensed by any third party to the Customer by reason of this Agreement and the Supplier acknowledges that all such Intellectual Property Rights remain the property of the Customer and/or its licensors.

10. **NO BRIBERY**

10.1. The Supplier shall comply with the Foreign Corrupt Practices Act, 15 U.S.C. §78dd-2 (the "**FCPA**") and the UK Bribery Act 2010 (the "**UKBA**") and shall procure the compliance with the FCPA and the UKBA by its group companies, associates and each of their respective directors, employees, agents and intermediaries or any party that is carrying out a service for the Customer (each an "**Associated Person**").

10.2. The Supplier shall not, and shall procure that each Associated Person shall not, directly or indirectly, request, agree to receive or accept a financial or other in violation of his/her or its lawful duty or inducing him/her or it to exercise his/her or its influence to affect or influence any act or decision (including the improper performance of any function) of him, her or it or to obtain or retain business for the Customer. The Supplier shall notify the Customer in writing immediately if it becomes aware of any violation of the FCPA, UKBA or this Clause 10.

11. CUSTOMER AND CLIENT MATERIALS

11.1. Title to any property of the Customer or a client of the Customer provided to the Supplier for the performance of the Services shall remain with the Customer or its clients (as applicable).

11.2. Subject to reasonable prior notice, the Customer or its client shall be entitled to retake possession of their property at any time from the Supplier.

11.3. The Supplier shall keep any property of the Customer or any client of the Customer in its possession safe and shall not dispose of or part with possession of such without the Customer and its client's written consent, save as otherwise required for the performance of the Services.

11.4. The Supplier hereby waives any lien or other right that it might otherwise have over any property of the Customer or a client of the Customer and shall keep the same free of all liens and other encumbrances.

11.5. The Supplier shall only use the property of the Customer or any client of the Customer in connection with the performance of the Services to which they relate.

12. MODERN SLAVERY ACT

12.1. The Supplier warrants that:

12.1.1. neither the Supplier nor any of its officers, employees, agents or subcontractors has:

(a) committed an offence under the Modern Slavery Act 2015 (a "**MSA Offence**");

(b) been notified that it is subject to an investigation relating to an alleged MSA Offence or prosecution under the Modern Slavery Act 2015;

(c) is aware of any circumstances within its supply chain that could give rise to an investigation relating to an alleged MSA Offence or prosecution under the Modern Slavery Act 2015;

12.1.2. it shall comply with the Modern Slavery Act 2015;

12.1.3. it shall notify Customer immediately in writing if it becomes aware or has reason to believe that it, or any of its officers, employees, agents or subcontractors have breached or potentially breached any of the Supplier's obligations under this clause 12.

13. GENERAL

13.1. The Supplier shall during this Agreement and for a period of 5 years thereafter, keep confidential all Confidential Information and shall not use or disclose such Confidential Information to any third party except as may be strictly necessary in order to perform the Services or as required by law.

13.2. Neither party may assign, subcontract or in any way transfer any of their rights or obligations under this Agreement without the prior written consent of the other party except that the Customer may assign its rights to any Affiliate.

13.3. Each provision of this Agreement is severable and distinct from the others. Invalidity or unenforceability of a specific

provision shall not affect the other provisions of this Agreement.

13.4. Any failure to exercise or any delay in exercising a right or remedy provided this Agreement or at law or in equity shall not constitute a waiver of the rights or remedies or a waiver of any other rights or remedies.

13.5. Nothing in this Agreement shall be construed as establishing or implying any partnership or agency relationship between the parties.

13.6. This Agreement constitutes the entire agreement and understanding between the parties in respect of the matters dealt with within it and supersedes any previous agreement between the parties relating to such matters. This Agreement may only be amended in writing with the agreement of the Customer and the Supplier.

13.7. No person who is not a party to this Agreement has any rights under the Contracts (Rights of Third Parties) Act 1999.

13.8. Any notice required to be given under this Agreement shall be in writing and shall be validly served only if sent to the other at the address on the Purchase Order by hand, by registered first class post or special delivery.

13.9. This Agreement and any noncontractual obligations shall be governed by English law and the parties agree to submit any dispute to the exclusive jurisdiction of the English Courts. The English Language version of this Agreement and any notice or other document relating to this Agreement, shall prevail if there is a conflict.

SCHEDULE 1 : KANTAR CODE OF BUSINESS CONDUCT

Kantar and its companies operate in many markets and countries throughout the world. In all instances, we respect national laws and any other laws with an international reach, such as the UK Bribery Act, the US Foreign Corrupt Practices Act and the UK Modern Slavery Act, where relevant, and industry codes of conduct. We are committed to acting ethically in all aspects of our business and to maintaining the highest standards of honesty and integrity.

We expect and require all our business partners, including suppliers, to have the same commitment to ethical behaviour and therefore ask you to confirm your agreement with our Code of Business Conduct (in the first column) as amended where necessary for non-Kantar entities (in the second column).

We expect all our suppliers to use appropriate systems to facilitate and monitor compliance with these standards and adherence to local and applicable international laws.

We expect our suppliers to demonstrate their commitment to the principles of this code and to have an on-going process of risk management to identify the environmental, health and safety, and labour practices and ethics risks associated with the suppliers' operations.

Suppliers should encourage staff to report concerns without fear of threat or reprisal. Suppliers should take appropriate action as required.

Suppliers should put in place equivalent standards to this Code for their own Supply Chain.

Kantar's Code	**What Kantar expects from its suppliers**
We, the officers and staff of all companies in the Kantar Group ("the **Group**"), recognise our obligations to all who have a stake in our success including share owners, clients, staff and suppliers.	You confirm that you recognise our obligations and will not act detrimentally to these obligations.
Information about our business shall be communicated clearly and accurately in a non-discriminatory manner and in accordance with local regulations.	You confirm that you will treat information about the Kantar Group as described.
We select and promote our people on the basis of their qualifications and merit, without discrimination or concern for race, religion, national origin, colour, sex, sexual orientation, gender identity or expression, age or disability.	You confirm that you have equivalent policies in your organisation.
We believe that a workplace should be safe and civilised and that employment must be freely chosen; we will not tolerate sexual harassment, discrimination or offensive behaviour of any kind, which includes the persistent demeaning of individuals through words or actions, the display or distribution of offensive material, or the use or possession of weapons on Kantar or client premises.	You confirm that you have equivalent policies in your organisation and for your supply chain, and that you will respect our workplace and people as described. In particular: • Employment must be freely chosen; forced or bonded labour or any other form of modern slavery must not be used; • Workers must not be forced to submit passports or government issued identities as a condition of employment; • Child labour is not to be used; • Compensation paid to workers must comply with all applicable wage laws;

	• Work weeks are not to exceed the maximum set by local law; • There is to be no inhumane treatment of workers including sexual harassment, sexual abuse, corporal punishment, physical coercion or verbal abuse; • Kantar expects its suppliers to create and foster safe working conditions for all workers; • Worker exposure to physical hazards must be eliminated wherever possible, or, if not, must be controlled; • Suppliers must have adequate procedures in place to handle emergencies that may affect workers; and • Systems must be in place to manage, track and report occupational injuries and illness.
We will not tolerate the use, possession or distribution of illegal drugs, or our people reporting for work under the influence of drugs or alcohol.	You confirm that you have equivalent policies in your organisation and that you will respect our workplace and people as described.
We will treat all information relating to the Group's business, or to its clients, as confidential. In particular, "insider trading" is expressly prohibited and confidential information must not be used for personal gain;	You confirm that you agree to our policy in respect of our information.
We are committed to protecting consumer, client and employee data in accordance with national laws and industry codes.	You confirm that you have equivalent commitments in your organisation that cover all information from and relating to our business and that of our partners in that business.
We will not knowingly create work which contains statements, suggestions or images offensive to general public decency and will give appropriate consideration to the impact of our work on minority segments of the population, whether that minority be by race, religion, national origin, colour, sex, sexual orientation, gender identity or expression, age or disability.	Wherever relevant, you confirm that you have equivalent standards for your work.
We will not undertake work which is intended or designed to mislead, including in relation to social, environmental and human rights issues.	Wherever relevant, you confirm that you have equivalent standards for your work.
We will consider the potential for clients or work to damage the Group's reputation prior to taking them on. This includes reputational damage from association with clients that participate in activities that contribute to the abuse of human rights.	This relates only to members of the Kantar Group.

We will not for personal or family gain directly or indirectly engage in any activity which competes with companies within the Group or with our obligations to any such company.	This relates only to members of the Kantar Group.
We will not give, offer or accept bribes, whether in cash or otherwise, to or from any third party, including but not restricted to government officials, clients and brokers or their representatives. We will collectively ensure that all staff understand this policy through training, communication and by example.	This applies directly to you.
We will not accept for our personal benefit goods or services of more than nominal value from suppliers, potential suppliers or other third parties.	This applies directly to you.
We will not have any personal or family conflicts of interest within our businesses or with our suppliers or other third parties with whom we do business.	You should have equivalent policies in your organisation.
No corporate contributions of any kind, including the provision of services or materials for less than the market value, may be made to politicians, political parties or action committees, without the prior written approval of the Kantar Board.	You should have your own policy regarding such contributions, together with appropriate authorisation procedures.
We will continue to strive to make a positive contribution to society and the environment by: maintaining high standards of marketing ethics; respecting human rights in our business, supply chain and through our client work; respecting the environment; supporting community organisations; supporting employee development; and managing significant sustainability risks in our supply chain. Our Sustainability Policy and Human Rights Policy Statement provide more detail about our commitments in these areas.	You should have equivalent policies in your organisation. In particular: • Suppliers must comply with the requirements of the UK's Modern Slavery Act; • Suppliers must obtain all relevant environmental authorisations, including for waste and emissions; • Suppliers must endeavour to prevent pollution by implementing conservation measures in their facilities and processes, by recycling, reusing and substituting materials.

We confirm that we adhere to the Kantar Code of Business Conduct as amended for our organisation. If we become aware of any breaches, particularly in respect of bribery or inappropriate gifts or services to or from your organisation or any other third party, or in respect of other matters that could harm Kantar's reputation directly or by association, we will inform you immediately.

Signature:

Name:

Position:

Organisation:

Date:

SCHEDULE 2 : INFORMATION SECURITY ADDENDUM

1. INTRODUCTION.

This Security Requirements Schedule (this "**Schedule**") establishes the basic requirements for Supplier's information security, as needed to ensure the confidentiality, availability and integrity of Customer Confidential Information and Customer's client's Confidential Information. Supplier shall comply with these requirements throughout Supplier's performance of services under this Agreement.

2. TERMINOLOGY

2.1. As used in this Schedule, each of the following terms (whether used with initial upper case or in all lower case) shall have the corresponding meaning set forth below. Each other capitalized term used herein but not defined herein shall have the meaning ascribed to it in this Agreement.

2.2. **Contractor** means a subcontractor, independent contractor, service provider or agent of Supplier that stores, processes, handles or has access to any Customer Confidential Information and Customer's client's Confidential Information.

2.3. **Customer Sensitive Information** means any Customer Confidential Information and Customer's client's Confidential Information that includes Personal Data [email, name etc.], health information, financial information or investment holdings information.

2.4. **Encryption** means the reversible transformation of data from the original (plaintext) to a obfuscated format (ciphertext) as a mechanism for protecting the information's confidentiality, integrity and/or authenticity. Encryption requires an encryption algorithm and one or more encryption keys.

2.5. **Store** means to store, archive, back-up and/or perform any similar activities.

3. SECURITY REVIEWS

3.1. Supplier shall provide Customer the right to an onsite review of Supplier's security program annually for the entire period that Supplier processes, stores or otherwise has access to Customer Confidential Information and Customer's client's Confidential Information. Supplier will promptly (but in no event later than thirty (30) days after receiving Customer's request to schedule and perform such review) schedule such review for a mutually agreeable date.

3.2. Supplier shall provide Customer with access to Supplier's Policies, procedures and other relevant documentation and to Supplier's Personnel as reasonably necessary to facilitate such reviews. Supplier shall file a remediation plan with Customer within thirty (30) days following the completion of such review, and Supplier shall remediate each such issue in a timely manner in accordance with a remediation schedule agreed to by the parties.

4. SPECIFIC SECURITY REQUIREMENTS

4.1. Security Policy

Supplier shall maintain a comprehensive set of written security policies and procedures which cover, at a minimum:

4.1.1. Supplier's commitment to information security;

4.1.2. information classification, labelling, and handling, and such policies and procedures related to information handling must describe the permissible methods for information transmission, storage, and destruction and such methods must be no less protective than those set forth in the Customer Supplier Information Protection Guidelines set forth below;

4.1.3. acceptable use of Supplier's assets, including computing systems, networks, and messaging;

4.1.4. information security incident management, including data breach notification and collection of evidence procedures;

4.1.5. authentication rules for the format, content and usage of passwords for end users, administrators, and systems;

4.1.6. access controls, including periodic reviews of access rights;

4.1.7. disciplinary measures for Supplier Personnel who fail to comply with such policies and procedures; and

4.1.8. the topics described in the remainder of this Section 4 in a manner consistent with the applicable requirements for such topics as set forth in this Section 4.

The supplier should notify Kantar of any fundamental changes to their policies within 30 days.

4.2. **Responsibility for Supplier's Information Security Program**

Supplier shall maintain an information security responsibility, with staff designated to maintain Supplier's information security program and to perform information security and information risk management.

4.3. **Audits, Review and Monitoring of Supplier's Information Security Program**

Supplier shall regularly monitor and review Supplier's information security program to ensure safeguards are appropriate to limit risks to Customer Confidential Information and Customer's client's Confidential Information.

4.4. **Asset and Information Management**

Supplier shall:

4.4.1. maintain an inventory of all Customer Confidential Information and Customer's client's Confidential Information that Supplier processes or stores;

4.4.2. maintain an inventory of physical computing and software assets Supplier uses in the performance of its activities under this Agreement; and

4.4.3. follow the Customer Supplier Information Protection Guidelines (set forth below) when handling, processing and storing Customer Confidential Information and Customer's client's Confidential Information.

4.5. **Physical and Environmental Security**

Supplier shall:

4.5.1. restrict entry to Supplier's area(s) where Customer Confidential Information and Customer's client's Confidential Information is stored, accessed, or processed solely to Supplier's Personnel authorized for such access;

4.5.2. implement reasonable best practices for infrastructure systems, including fire extinguishing, cooling, and power, emergency systems, and employee safety;

4.5.3. provide physical entry controls for all areas where Customer Confidential Information and Customer's client's Confidential Information is stored, accessed, or processed that are commensurate with the sensitivity of the Customer Confidential Information and Customer's client's Confidential Information;

4.5.4. regularly monitor areas where Customer Confidential Information and Customer's client's Confidential Information is handled, stored and/or processed

4.6. **Employee-related Matters**

Supplier shall:

4.6.1. Perform criminal background checks on each of Supplier's Personnel (including Contractors), where allowed by law, that has access to Customer Confidential Information and Customer's client's Confidential Information, except to the extent limited or prohibited by applicable laws; such background checks must be performed prior to allowing such individual to access Customer Confidential Information and Customer's client's Confidential Information and Supplier shall not allow any individual who does not have a satisfactory background check to access Customer Confidential Information and Customer's client's Confidential Information;

4.6.2. train its new personnel (including Contractors) on the acceptable use and handling of Supplier's confidential information and confidential information of other companies that has been entrusted to Supplier (such as Customer Confidential Information and Customer's client's Confidential Information);

4.6.3. provide security and data privacy education and training for its personnel (including Contractors) and maintain a record of personnel that completed such education; and

4.6.4. implement a formal user registration and de-registration procedure for granting and revoking access to Supplier's information systems and services; and upon termination of any of Supplier's Personnel (including Contractors), Supplier shall revoke such individual's access to Customer Confidential Information and Customer's client's Confidential Information as soon as possible but in no event later than two (2) Working Days following termination of such individual.

4.7. **Communications and Operations**

Supplier shall:

4.7.1. perform regular backups sufficient to restore services to Customer within the agreed upon recovery times (or, if no specific recovery times have been agreed to by the parties, within a commercially reasonable period of time);

4.7.2. encrypt all backup media containing Customer Confidential Information and Customer's client's Confidential Information in accordance with the Customer Supplier Information Protection Guidelines set forth below;

4.7.3. not store or replicate any Customer Confidential Information and Customer's client's Confidential Information outside of Supplier's premises without obtaining the prior written consent of Customer;

4.7.4. not transmit, transfer or provide any Customer Confidential Information and Customer's client's Confidential Information to any third party, or provide any third party with access to any Customer Confidential Information and Customer's client's Confidential Information, without obtaining the prior written consent of Customer;

4.7.5. if any activities described in the previous clauses 4.7.3 and 4.7.4 are approved by Customer, maintain an inventory of the third parties and/or locations outside of Supplier's premises that store or replicate any Customer Confidential Information and Customer's client's Confidential Information, the third parties that receive or receive access to Customer Confidential Information and Customer's client's Confidential Information, the purpose for storing, replicating, providing or providing access to such Customer Confidential Information and Customer's client's Confidential Information, the manner in which such Customer Confidential Information and Customer's client's Confidential Information was transmitted or otherwise provided to such third party, the transmission and encryption/protection

method or protocol (where applicable) used in transmitting or otherwise providing such Customer Confidential Information and Customer's client's Confidential Information, a description of the Customer Confidential Information and Customer's client's Confidential Information that was transmitted or otherwise provided to such third party, the name of the Customer employee that approved such arrangement and the date such approval was obtained;

4.7.6. when erasing or destroying Customer Confidential Information and Customer's client's Confidential Information, employ data destruction procedures that meet or exceed the Department of Defence Standard for Secure Data Sanitization (DOD 5220.22M). Supplier shall promptly erase or destroy any or all Customer Confidential Information and Customer's client's Confidential Information upon written request from Customer;

4.7.7. follow the Customer Supplier Information Protection Guidelines set forth below, including those pertaining to encryption, when transmitting or transporting Customer Confidential Information and Customer's client's Confidential Information;

4.7.8. use hard drive encryption for all mobile devices on which any Customer Confidential Information and Customer's client's Confidential Information is stored or that are used by Supplier's Personnel to access any Customer Confidential Information and Customer's client's Confidential Information, and such encryption shall be in accordance with the Customer Supplier Information Protection Guidelines set forth below;

4.7.9. maintain up to date malware detection and prevention on Supplier's servers and/or end user platforms that transmit, access, process or store Customer Confidential Information and Customer's client's Confidential Information;

4.7.10. maintain a hardened Internet perimeter and secure infrastructure using firewalls, antivirus, anti-malware, intrusion detection systems, and other protection technologies as is commercially reasonable; and

4.7.11. implement regular patch management and system maintenance for all of Supplier's systems that transmit, access, process or store Customer Confidential Information and Customer's client's Confidential Information.

4.8. **Access Control**

Supplier shall:

4.8.1. enforce best practices for user authentication; if passwords are used to authenticate individuals or automated processes accessing Customer Confidential Information and Customer's client's Confidential Information, such passwords will comply with the current best practices for password usage, creation, storage, and protection. (Refer to the Customer Supplier Information Protection Guidelines below).

4.8.2. ensure that user IDs are unique to individuals and are not shared and removed within 48 hours of a users termination with the Supplier;

4.8.3. assign access rights based upon the sensitivity of Customer Confidential Information and Customer's client's Confidential Information, the individual's job requirements, and the individual's "need to know" for the specific Customer Confidential Information and Customer's client's Confidential Information;

4.8.4. review the access rights of Supplier's Personnel (including Contractors) at least annually to ensure need-to-know restrictions are kept current;

4.8.5. regularly review reports of user entry into Supplier's facilities housing Customer Confidential Information and Customer's client's Confidential Information; and

4.8.6. not leave Customer Confidential Information and Customer's client's Confidential Information unattended on desktops, printers or elsewhere in an unsecure manner in Supplier's facilities.

4.9. **Application Development; Vulnerability Scans and Penetration Tests**

Supplier shall:

4.9.1. implement a secure development methodology that incorporates security throughout the development lifecycle;

4.9.2. develop and enforce secure coding standards;

4.9.3. perform secure code reviews using automated scanning tools for all externally-facing applications and for any software developed by Supplier (or a Contractor) and delivered to Customer;

4.9.4. perform vulnerability scans at least once each quarter for all externally-facing applications that receive, access, process or store Customer Confidential Information and Customer's client's Confidential Information; upon request by Customer, Supplier shall confirm in writing that Supplier has successfully performed such vulnerability scans;

4.9.5. use an external third party security testing company to perform penetration tests at least once each year for all externally-facing applications that receive, access, process or store Customer Sensitive Information; such penetration tests shall be conducted by Supplier's testing vendor who has been approved by Customer; upon request by Customer, Supplier shall confirm in writing that Supplier has successfully performed such penetration tests; and Supplier shall correct all material issues discovered in the course of such penetration tests conducted by or on behalf of Supplier within thirty (30) days or, if such issue(s) cannot be corrected within such thirty (30) day period, within a period of time mutually agreed to by Supplier and Customer.

4.10. **Contractors**

Supplier shall:

4.10.1. take reasonable steps to select and maintain Contractors that are capable of maintaining security measures to protect Customer Confidential Information and Customer's client's Confidential Information in accordance with applicable laws and regulations and in a manner no less protective than the requirements set forth in this Agreement, including this Schedule; and maintain with each such Contractor a written contract requiring such Contractor, by contract, to implement and maintain such security measures;

4.10.2. not provide to any Contractor, or allow any Contractor to access, process, store, view or otherwise interact with, any Customer Confidential Information and Customer's client's Confidential Information without obtaining the prior written consent of Customer;

4.10.3. be responsible to Customer for all acts and omissions of any Contractor, including any failure by a Contractor to comply with the provisions of this Agreement, including this Schedule; and

4.10.4. perform on a regular basis a review of each Contractor that includes a review of Contractor's information security policies and practices.

5. **INFORMATION SECURITY INCIDENT MANAGEMENT**

5.1. Supplier shall:

5.1.1. establish, test, and maintain an information security incident response process that includes, among other things, processes for evidence preservation, informing and working with law enforcement agencies, government agencies and similar parties as appropriate, and performing forensic analyses;

5.1.2. notify Customer in writing of any information security breach involving Customer Confidential Information and Customer's client's Confidential Information, including any actual or suspected unauthorized access to Customer Confidential Information and Customer's client's Confidential Information or a security incident at or involving a Contractor's systems, hardware, equipment, devices or premises computers or otherwise involving a Contractor's personnel; Supplier shall provide notification of any such incident promptly, but in no event later than twenty-four (24) hours following the date Supplier first becomes aware of such incident. Thereafter, Supplier shall provide regular updates to Customer regarding the investigation and mitigation of such event. Supplier shall permit Customer or its designees to participate in all aspects of the investigation. Supplier shall be responsible for all costs incurred by any party connection with such incidents, including but not limited to, notification to affected Data Subjects, forensic investigations, credit monitoring for Data Subjects and other remedial and legal efforts; and

5.1.3. for each such incident, provide Customer with a final written notification no later than ten (10) days following Supplier's closure of such incident, that includes detailed information regarding the root cause of such incident, actions taken, and plans to prevent a similar event from occurring in the future.

6. BUSINESS CONTINUITY MANAGEMENT

6.1. Supplier shall:

6.1.1. establish and maintain a comprehensive business continuity plan ("**BCP**") that covers the restoration of both technology and business operations in the event of an unplanned event;

6.1.2. test or review its BCP at least annually in a manner it deems appropriate in its sole and absolute discretion.

7. COMPLIANCE

7.1. Supplier shall:

7.1.1. comply with the Customer Supplier Information Protection Guidelines set forth below;

7.1.2. establish and maintain mutually agreed upon policies and practices for records retention and data destruction applicable to the Customer Confidential Information and Customer's client's Confidential Information and any other information produced in the course of or otherwise related to Supplier's activities under this Agreement;

7.1.3. establish a code of ethics and require employees to review and acknowledge it annually (except if and to the extent prohibited by law).

8. FOLLOW-UP RISK MANAGEMENT ACTIONS

8.1. If Customer has previously performed a security review of Supplier and/or one or more of its facilities (or those of its Contractors, as applicable), and as a result of such security review, items of concern were identified by Customer, Supplier shall:

8.1.1. if it has not already done so, reasonably cooperate with Customer to promptly develop a mutually agreeable risk management plan to remediate such items of concern, and

8.1.2. implement the actions specified in the risk management plan no later than the corresponding date set forth in such risk management plan.

8.2. The risk management plan for the most recent security review is set forth below, or, if the plan below is blank, shall be set forth in another document prepared and agreed to by the parties.

RISK MANAGEMENT PLAN		
Level of Concern	Action Plan	Date
HIGH		
MEDIUM		
LOW		

9. **IDENTITY THEFT**

If Supplier processes, handles or has access to Personal Data, Supplier shall promptly notify Customer if, during the course of Supplier's activities under this Agreement, Supplier's employees become aware of any potential identity theft related to the individual(s) to which such Personal Data relates.

10. **UPDATES**

Customer may update this Information Security Addendum at any time upon thirty (30) days prior written notice to Supplier. In the event that Supplier believes that it cannot comply with such updates, Supplier shall notify Customer in writing within such thirty (30) day period setting forth the specific items for which Supplier cannot meet. In such event, Customer reserves the right to terminate any or all services or projects with Supplier without liability or penalty on account of such termination.

ANNEX 1

CUSTOMER SUPPLIER INFORMATION PROTECTION GUIDELINES

Customer Information Classification and Handling Matrix

Without limiting Supplier's obligations as set forth in this Agreement, including this Schedule, the table below summarizes certain specific requirements applicable when transmitting (or transferring), storing or destroying Customer Confidential Information and Customer's client's Confidential Information, including Customer Sensitive Information.

Information Classification	Examples	Transmission	Storage	Destruction
Customer Confidential Information and Customer's client's Confidential Information other than Customer Sensitive Information	Business strategies and plans; Audit reports; Pre-release marketing information; Customer proprietary software; Technical specifications or architectures	Electronic: Encrypt when transmitted over public networks or transferred outside of Supplier's premises on portable media or devices or other electronic media; Print: Send via courier (including overnight delivery service) or registered mail with tracking number.	Limit accessto authorized personnel only; perform quarterly access rights reviews. Encryption when in storage preferred.	Electronic: Use DOD 5220.22M or equivalent procedures. Print: Shred
Customer Sensitive Information	Personal Data (including name, email, phone, mailing address, SSN, or account number) Personal financial information Personal health information	Same as above	Limit access to authorized personnel only; perform quarterly access rights reviews. Encryption in storage required.	Same as above

Encryption

Set forth below are Customer's current preferred encryption algorithms and current additional acceptable encryption algorithms. Supplier shall use one of the preferred encryption algorithms when encrypting Customer Confidential Information and Customer's client's Confidential Information unless it is not reasonably feasible to do so, in which case Supplier shall use one of the additional acceptable encryption algorithms when encrypting Customer Confidential Information and Customer's client's Confidential Information.

Preferred Encryption Algorithms		
Purpose	**Algorithms**	**Minimum Key Length (Bits)**
Key Exchange	RSA Diffie-Hellman	2048 preferred, if not

		possible then 1024
Data Protection	AES in CBC mode 3DES in CBC EDE3 mode	256 preferred, if not possible then 128 168
Hash	SHA-256	N/A
HMAC	HMAC SHA-256	256
Digital Signature	RSA with SHA-256 DSA with SHA-256	2048 preferred, if not possible then 1024

Additional Acceptable Encryption Algorithms		
Purpose	**Algorithms**	**Minimum Key Length (Bits)**
Data Protection	AES in CTR mode RC4 RC5 in CBC mode Blowfish in CBC mode CAST-128 in CBC mode IDEA in CBC mode	2048 preferred, if not possible then 128
Hash	SHA-2 preferred, if not possible then SHA-1 MD5 should never be used unless an exception for technology is needed.	N/A
HMAC	HMAC SHA-2 preferred, if not possible then SHA-1 MD5 should never be used unless an exception for technology is needed.	160 128
Digital Signature	ECC with SHA-256, SHA-2 RSA with SHA-2 preferred, if not possible then SHA-1, DSA with SHA-2 preferred, if not possible then SHA-1	160 min 2048 preferred, if not possible then 1024

Password-based Authentication Guidelines

All passwords administered or controlled by Supplier (or a Contractor) shall meet the following guidelines:

Area	**Guideline**
Minimum password length	8 characters
Password complexity	2 of the 4 character types (upper, lower, digits, special), not be easily associated with an individual or process, not found in a dictionary and not

	represent a pattern. It is strongly recommended that passwords contain 3 of the 4 character types
Maximum password lifetime	At most 90 days
Minimum password history	1 day
Protection in transit	Mandatory: Passwords must be encrypted in transit.
Protection in storage	Mandatory: Passwords must be hashed using an approved hash algorithm (see table above).

SCHEDULE 3

DATA PROTECTION

1. **DEFINITIONS**

1.1. In this Schedule 3 terms used but not otherwise defined in this Agreement have the meanings given in the GDPR.

1.1.1. **In-Scope Personal Data** means any Personal Data that is processed by the Supplier in the course of providing the Services or performing its other obligations under this Agreement;

1.1.2. **Data Safeguards** means administrative, technical and physical safeguards that protect against threats or hazards to the integrity and security of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to, In-Scope Personal Data and that comply with best industry practice;

1.1.3. **Model Terms** means the standard contractual clauses approved by European Commission decision of 5 February 2010 (2010/87/EU) on standard contractual clauses for the transfer of Personal Data to Processors established in third countries (but which shall exclude any contractual clauses designated by the European Commission as optional in that decision), as amended or replaced from time to time by the European Commission;

1.1.4. **"Sub-processor"** means any third party appointed by Supplier to Process In-Scope Personal Data on behalf of Customer in connection with the Agreement;

1.1.5. The terms, **"Controller", "Data Subject", "Member State", "Personal Data", "Processing", "Processor"**, and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly; a reference to transferring data out of any country or territory includes, without limitation, remotely accessing that data from outside that country or territory;

1.1.6. the reference to "applicable laws" in Clause 2.4 of the Agreement shall be limited to European Union or Member State law to which the Supplier is subject, to the extent that those Clauses apply in relation to In-Scope Personal Data the Processing of which is subject to European Union or Member State law.

2. **OBLIGATIONS**

2.1. Each of the Supplier and Customer shall, at all times, comply with its obligations under all Data Protection Legislation and all applicable Supplier Policies in connection with this Agreement.

2.2. The Supplier shall not be entitled to use or otherwise process any In-Scope Personal Data for any purpose other than to provide the Services and to perform its other obligations under this Agreement.

2.3. Roles of the Parties. The parties acknowledge and agree that with

regard to the Processing of In-Scope Personal Data, Customer is the Controller, Supplier is the Processor and may only engage Sub-processors pursuant to the requirement set forth in section 2.8.2(b) below.

2.4. The Supplier shall:

2.4.1. process In-Scope Personal Data only on and in accordance with the written instructions of Customer;

2.4.2. promptly notify Customer upon becoming aware of any errors or inaccuracies in any In-Scope Personal Data;

2.4.3. ensure that, except as otherwise instructed in writing by Customer or required by Data Protection Legislation, any copies of In-Scope Personal Data in the possession or under the control of the Supplier, any Sub-processor or any Supplier Personnel are permanently destroyed when they are no longer required for the performance of the Supplier's obligations under this Agreement;

2.4.4. ensure that In-Scope Personal Data is accessible only to Supplier Personnel who:

(a) need to have access to the data in order to carry out their roles in the performance of the Supplier's obligations under this Agreement;

(b) have been appropriately trained on the requirements of Data Protection Legislation applicable to the Processing, care and handling of the data; and

(c) are subject to contractual or statutory obligations of confidentiality in respect of the In-Scope Personal Data; and

2.4.5. subject to Clause 2.15, give the Customer such co–operation, assistance and information and execute all documents as they may reasonably request to assist them to comply with their obligations under any Data Protection Legislation insofar as they relate to any In-Scope Personal Data, and co–operate and comply with the directions or decisions of any Supervisory Authority in relation to such data, and, in each case, within such time to assist Customer and to meet any time limit imposed by Data Protection Legislation or by the Supervisory Authority.

2.5. In respect of In-Scope Personal Data the Processing of which is subject to European Union or Member State law, the Supplier shall:

2.5.1. not transfer, and shall ensure that any Sub-processor does not transfer, such data out of any country or territory, nor require any Customer to make such a transfer, except:

(a) between member states of the European Union, the European Economic Area;

(b) on the written instructions of Customer, and then subject to any

reasonable additional restrictions set by Customer and at any time in relation to a transfer of this kind promptly enter into (or require, in the case of a transfer by or to a Sub-processor, that that Sub-processor promptly enters into) an agreement with Supplier on Model Terms unamended but completed in such manner as Customer may reasonably stipulate, or such other form as the Parties may agree in writing.

2.6. In respect of In-Scope Personal Data not falling within Clause 2.5, but the Processing of which is subject to any Data Protection Legislation that prohibits or restricts

2.6.1. the transfer of that In-Scope Personal Data to any country or territory or

2.6.2. the Processing of that In-Scope Personal Data in any country or territory, the Supplier shall not transfer or process that In-Scope Personal Data in contravention of any such prohibition or restriction.

2.7. The Supplier shall:

2.7.1. at all times have in place (and keep Customer's data protection officer informed in writing of the identity of) a Supplier Personnel who is responsible for assisting Customer in responding to enquiries received from Data Subjects or any Supervisory Authority;

2.7.2. ensure that the Supplier Personnel referred to in Clause 2.7.1 always responds promptly and reasonably to the enquiries referred to in that Clause, taking full account of the relevant requirements of Data Protection Legislation as to timely response; and

2.7.3. take no steps in relation to any enquiry as referred to in Clause 2.7.1 except on the written instructions of the applicable Customer.

2.8. The Supplier shall:

2.8.1. not disclose or transfer any In-Scope Personal Data to any third party, except for a disclosure or transfer:

(a) made on the written instructions of Customer and in accordance with Clause 2.5;

(b) to the extent required by Data Protection Legislation or any other provision of this Agreement;

2.8.2. in respect of any processing of In-Scope Personal Data by a Sub-processor:

(a) comply with the provisions of Clause 13.2 of the Agreement, (Assignment, Subcontracting);

(b) ensure that the Sub-processor's processing is carried out under a written contract imposing on the Sub-processor the same obligations as are imposed on the Supplier under this Schedule 3 (Data Protection: GDPR);

(c) procure that the Sub-processor performs and observes those obligations; and

(d) if Customer so requests, procure that the Sub-processor enters into a written contract with Customer, imposing on the Sub-processor the same obligations as are imposed on the Supplier under this Schedule 3 (Data Protection).

2.9. The Supplier:

2.9.1. shall adopt, implement and maintain Data Safeguards, including, as part of the Data Safeguards, security procedures and practices to prevent the unauthorized or accidental access to or destruction, loss, modification, use or disclosure of In-Scope Personal Data;

2.9.2. warrants to Customer that the Supplier has written security policies, procedures and practices that comply with the Supplier's data security obligations under Data Protection Legislation;

2.9.3. shall maintain and enforce the Data Safeguards at each facility from which the Supplier provides the Services, and with respect to any and all networks that process In-Scope Personal Data; and

2.9.4. shall review and revise the Data Safeguards from time to time in accordance with prevailing industry practices and as reasonably requested by Customer (and shall promptly provide details of such revised Data Safeguards to Customer in writing upon request).

2.10. In the event of any unauthorized or accidental access to or use or disclosure of any In-Scope Personal Data, or the Supplier having reasonable belief that any such access, use or disclosure has occurred or is at risk of occurring (which shall include, without limitation, the loss of or the inability to locate definitively any media, device or equipment on which In-Scope Personal Data is or may be stored), the Supplier shall:

2.10.1. notify Customer without delay, and in any event within twenty-four (24) hours, providing reasonable detail of the impact on Customer of the access, use or disclosure and the corrective action taken and to be taken by the Supplier;

2.10.2. subject to Clause 2.15, promptly take all necessary and appropriate corrective action to remedy the underlying causes of the access, use or disclosure;

2.10.3. take any action pertaining to the access, use or disclosure required by Data Protection Legislation including, without limitation, at the request of Customer, providing notices to data subjects whose personal data may have been affected, whether or not such notice is required by Data Protection Legislation; and

2.10.4. if the access, use or disclosure would permit access to a data subject's financial information or lead to a reasonable risk of identity theft or fraud, the Supplier shall provide, for a

reasonable period of time of not less than one (1) year, credit monitoring services for any such data subjects.

2.11. In addition to any audit rights within the Agreement and upon request by Customer and subject to Customer's reasonable discretion, Supplier allows Customer (either on its own or on behalf of its clients) or an independent auditor instructed by Customer to audit and review the Supplier's, and the approved Sub-Processor's, information security program, data processing facilities and data protection compliance program in order to verify compliance with this Schedule 3 (Data Protection), Data Protection Legislation and Customer or Customer's own clients' obligations, ("**Data Protection and Security Audit**").

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

2.13. If the Customer reasonably believes that the results of a Data Protection and Security Audit identifies a weakness in the security measures adopted by the Supplier, or the approved Sub-Processor, the Supplier shall evaluate such weakness and provide a suitable solution to the Customer's satisfaction within timescales agreed by the Customer.

2.14. The Supplier acknowledges that any regulator or its agent may from time to time audit the Supplier, or any approved Sub-Processors, and that any such audit shall not be subject to any of the restrictions set out in these Clauses 2.11 to 2.14.

2.15. Customer:

2.15.1. is responsible, in its own right for instructing the Supplier to take such steps in the Processing of Personal Data on behalf of Customer as are reasonably necessary for the performance of the Supplier's obligations under this Agreement; and

2.15.2. authorizes the Supplier, to the extent permitted by Data Protection Legislation, to provide equivalent instructions to the Sub-processors on behalf of Customer.

2.16. The costs and expenses incurred by the Supplier in complying with Clauses 2.4.5, 2.10.2, 2.10.3 and 2.10.4 shall be borne:

2.16.1. by the Supplier in cases where the action required to be taken by the Supplier results from a breach of this Agreement or any negligent, wilful or fraudulent act or omission of the Supplier including failure to comply with the GDPR, any Sub-processor or any Supplier Personnel; and

2.16.2. by Customer in other cases.

2.17. Supplier shall, at any time on the request of Customer, return all Personal Data of which Customer is the sole Controller, and which is Processed by Supplier on behalf of Customer under the Agreement, to Customer and/or at Customer's request delete the same from its systems, other than any back-up copies which Supplier or its Affiliates are required to retain for compliance with applicable laws or regulatory requirements provided that such copies are kept confidential and secure in accordance with this Schedule 3 (Data Protection).

KANTAR

Signed for and on behalf of the Supplier

SIGNED _____

NAME _____

POSITION _____

SUPPLIER NAME _____

DATED _____