HURON

DATA PROCESSING AND SECURITY ADDENDUM

This Data Processing and Security Addendum ("DPSA") is incorporated into and made a part of the Agreement between Company and Contractor. Nothing in this DPSA limits or restricts Company's rights or Contractor's obligations under the Agreement in relation to the protection of Personal Information or permits Contractor to Process (or permit the Processing of) Personal Information in a manner which is prohibited by the Agreement. Terms not defined herein shall have the meaning set forth in the Agreement. In the event of a conflict between the DPSA and Agreement, the terms and conditions of the DPSA shall prevail.

Contractor will provide services as described in the Agreement and any statements of work thereto (the "Services") which will involve the Processing of Personal Information (defined below). All Company Data (defined below) shall be deemed "Confidential Information" under the Agreement.

1. **Definitions.** In this DPSA, the following definitions shall apply. All other capitalized terms should have the meaning ascribed by the Data Protection Laws:

a. "**Company Data**" means any Company non-public or proprietary information and data in any form, including Personal Information, provided by Company and its authorized agents or subcontractors or otherwise Processed by Contractor Personnel in connection with the provision of Services under the Agreement.

b. **"Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information. Controller may also be referred to as "**Business**" under applicable Data Protection Laws.

c. "**Data Protection Laws**" means all applicable laws with respect to Personal Information Processed by Contractor.

d. "**Data Subject**" means the individual to whom Personal Information relates. Data Subject may also be referred to as "**Consumer**" under applicable Data Protection Laws.

e. **"De-Identified Data"** means information that cannot be reasonably used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to an individual.

f. "**Personal Information**" means any information relating to an identified or identifiable natural person, consumer, or household, either directly or indirectly. Personal Information may also be referred to as "**Personal Data**" under applicable Data Protection Laws.

g. **"Personal Information Breach**" means the theft or unauthorized or unlawful loss, destruction, access, use, disclosure, or modification of, or inability to access (including encryption of) any Personal Information. Personal Information Breach may also be referred to as a "**Personal Data Breach**" under applicable Data Protection Laws.

h. "**Processing**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

i. "**Processor**" means any third party appointed by a party to Process Personal Information in relation to this DPSA on behalf of that party. Processor may also be referred to as "**Contractor**" or "**Service Provider"** under applicable Data Protection Laws.

j. "**Restricted Transfer**" means any transfer of Personal Information that would be prohibited by Data Protection Laws in the absence of legally required safeguards.

k. "**Sub-processor**" means any third party appointed by Contractor to Process Personal Information in relation to this DPSA on behalf of the Company. "**Sub-processor**" may also be referred to as "**Subcontractor**" under applicable Data Protection Laws.

2. Processing of Personal Information.

a. **Role of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Information, the Company is the Controller, and the Contractor is the Processor, or equivalent terms in the applicable Data Protection Laws.

b. **Contractor Obligations.**

i. Contractor shall comply at all times with the Data Protection Laws and this DPSA, and Contractor's performance under this DPSA shall not, in any event, cause the Company to be in violation of any Data Protection Laws. In the event of a claim against Contractor alleging violation of a country-specific Personal Data Law, Contractor agrees to submit to a court of competent jurisdiction.

ii. As between the parties, all Company Data remains, at all times, the property of Company, and Company has the right to direct Contractor in connection with Contractor's Processing of such Company Data.

iii. Contractor shall Process the Personal Information only (1) on and in accordance with the documented instructions of the Company; or (2) to the extent permitted by applicable law, provided that Contractor promptly inform the Company in writing of any such legal requirement, unless not legally permitted to do so.

iv. The Company instructs Contractor to Process Personal Information as reasonably necessary for the provision of the Services and consistent with the Agreement. Contractor will notify the Company if it is or believes it will be unable to

comply with the terms of this DPSA, the instructions of the Company, the relevant Data Protection Laws, or changes in legislation applicable to Contractor or a Sub-processor likely to have a substantial effect on the obligations in this DPSA. In such case, Contractor will, in consultation with the Company, take reasonable and appropriate steps to address and remediate such potential non-compliance, promptly cease any unauthorized Processing, and shall not at any event undertake any additional Processing that is in breach of this DPSA, the instructions of the Company, or the Data Protection Laws.

v. Contractor shall promptly notify Company of any inquiries or complaints received about the Processing of Company Data from third parties, including regulators, individual Data Subjects, and law enforcement. Contractor shall not respond to any such inquiries or complaints except on the documented instruction of Company or as required by law. If Company responds or allows the response to an inquiry or complaint, Contractor shall provide Company with reasonable cooperation and assistance in responding to any such inquiry, or complaint, including requests by individuals to amend, transfer, delete, or exercise other individual Data Subject rights around Personal Information.

vi. Contractor shall maintain records of Processing activities for the Processing of Personal Information, carried out pursuant to this DPSA, containing all relevant details required by Data Protection Laws.

vii. Where Contractor Processes Personal Information as that term is defined in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CPRA") (collectively, the "CCPA"), Contractor shall not: (a) Sell or Share (as those terms are defined in the CCPA) Personal Information; (b) retain, use, or disclose the Personal Information for any purpose other than the specific purpose of providing the Services specified in the Agreement, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the Services specified in the Agreement, except as explicitly permitted by the CCPA; (c) retain, use, or disclose the Personal Information outside of the direct business relationship between Contractor and the Company; and/or (d) combine the Personal Information Contractor receives pursuant to the Agreement with Personal Information which Contractor receives from or on behalf of another person or persons, or that Contractor may collect from its own interaction with the consumer unrelated to this Agreement, provided that Contractor may combine Personal Information solely if required to perform any business purpose as described in CCPA § 1798.140.

c. **Details of Processing.** Exhibit A describes Contractor's Processing activities. The Company may make reasonable amendments to Exhibit A as the Company reasonably considers necessary.

d. **Disclosure.** If Contractor is (1) required by Data Protection Laws to disclose any Personal Information to a governmental authority; or (2) subject to an investigation, enquiry or inspection by a governmental authority, Contractor shall (i) provide prior written notice to the Company within twenty-four (24) hours of receipt of the governmental authority request and that notice shall include a copy of the request and any related documents; and (ii) not disclose such Personal Information or provide any responses, information or documents to the governmental authority in question without the Company's prior written approval, and only comply with provision of the minimum amount of Company Data required.

e. **Deidentified Data.** In the event that the Company shares Deidentified Data with Contractor, Contractor warrants that it: (1) takes reasonable measures to ensure that the information cannot be associated with a consumer or household; (2) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and (3) contractually obligates any recipients of the information to comply with all provisions of applicable Data Protection Laws with respect to the information.

f. **Annexes.** To the extent that Contractor collects Personal Information subject to Data Protection Laws identified in the Annexes attached to this DPSA, Contractor will comply with the relevant Annex when processing such Personal Information. In the event of a conflict between the body of this DPSA and any Annex, the applicable Annex shall govern as to the Personal Information processed in scope of that Annex.

3. Personnel. Contractor will:

a. Strictly limit access to Personal Information to only those employees, agents, or contractors who need to know and access the relevant Personal Information to provide the Services; and

b. Confirm that such employees, agents, or contractors are subject to confidentiality obligations and are required at all times to comply with this DPSA, the Company's instructions, and Data Protection Laws. For the avoidance of doubt, Contractor remains fully liable to the Company for the actions and omissions of any of Contractor's or Sub-processors' employees, agents, and contractors.

4. Data Security.

a. Contractor will implement and maintain administrative, physical, technical, and operational safeguards based upon risk assessment for the protection of the security, confidentiality, and integrity of Company and Personal Information, as provided by this DPSA and Data Protection Laws, including without limitation those technical and organizational measures referred to in Exhibit B to this DPSA. Contractor shall monitor developments in technology and security to confirm that the measures implemented pursuant to this clause remain up to date and appropriate and will assist the Company in fulfilling its obligations in relation to the security of processing of Personal Information.

b. In assessing the appropriate level of security, Contractor shall take into account in particular the risks that are presented by Processing, especially Personal Information, and match the measures it applies to its own equivalent of data.

c. Contractor shall document its data security program in written form and shall make those documents available to the Company for review upon the Company's request.

5. Sub-processing.

a. Contractor will not engage or use any Sub-processor without the Company's prior written consent. The Company authorizes Contractor to appoint those Sub-processors that are already used by Contractor and listed in Exhibit C to this DPSA.

b. With respect to each Sub-processor, Contractor shall:

i. Before the Sub-processor first Processes Personal Information, carry out adequate due diligence to confirm that the Sub-processor is capable of providing the level of protection for Personal Information required by this DPSA and implements data security measures substantially similar to those in Exhibit B and as otherwise required by Data Protection Laws;

ii. Enter a written contract with each Sub-Processor and confirm that each contract it enters into with Sub-processors, to the extent they have access to Personal Information, has terms that are materially and substantively consistent with this DPSA such that each Sub-processor will comply with the applicable terms of this DPSA;

iii. Provide to the Company for review copies of such contracts with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPSA) as the Company may request from time to time;

iv. At no charge to the Company, actively monitor, regularly audit and, where applicable, take steps to enforce compliance of Sub-processors with their obligations under this DPSA, reporting promptly to the Company any detected or reported non-compliance and all actions taken to remedy the same. If a Sub-processor fails to remedy non-compliance within a reasonable time after notice from Contractor, the Company shall be entitled, without prejudice to any other right or remedy, to require Contractor to cease using the corresponding Sub-processor and resume the provision of that part of the Services itself; and

v. Be fully responsible and liable to the Company for any acts or omissions of Sub-processors as if they were Contractor's own.

6. Data Subject Rights.

a. Contractor will assist the Company as necessary for the fulfilment of the Company's obligations under the Data Protection Laws to effectively respond to requests from Data Subjects exercising their rights relating to Personal Information.

b. Contractor shall promptly, and in any event within forty-eight (48) hours, notify the Company if Contractor receives a Data Subject request in respect of Personal Information, and will not respond to that request except on the documented instructions of the Company.

7. Breach of Data Protection Laws. If Contractor becomes aware of its actual or suspected breach of Data Protection Laws relating to the Personal Information, then it shall immediately, and in any event not later than twenty-four (24) hours upon becoming aware of this breach, report the breach to the Company and, if requested, assist the Company in meeting any obligations under the Data Protection Laws.

8. Personal Information Breach.

a. If Contractor has knowledge of any actual or suspected Personal Information Breach, it shall:

i. Report to the Company, including by telephone to Contractor's primary business contact and via email to Huron-GDPR-Team@hcg.com such actual or suspected Personal Information Breach to the Company immediately, and in any event not later than twenty-four (24) hours upon becoming aware of the actual or suspected Personal Information Breach, providing the Company with sufficient information to allow the Company to meet any and all obligations imposed by Data Protection Laws, including, but not limited to the obligations to report such Personal Information Breach to a regulatory authority and to inform Data Subjects of the Personal Information Breach;

ii. At a minimum: describe the nature of the Personal Information Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of data records concerned; the name and contact details of Contractor's DPO and/or other contact from whom information can be obtained; describe the likely consequences of the Personal Information Breach; and describe the measures taken or proposed to be taken to address the Personal Information Breach;

iii. Mitigate any harmful effects of such Personal Information Breach; and

iv. Cooperate with the Company in providing any notices to the competent regulatory or supervisory authority and the Data Subjects that the Company deems appropriate.

b. Contractor will not inform any third party of a Personal Information Breach without the prior, written consent of the Company, unless required by Data Protection Laws, in which case, to the extent permitted by such law, Contractor shall inform the Company of that legal requirement, provide a copy of the proposed notification, consider any comments made by the Company before notifying any third party of the Personal Information Breach, and receive Company consent to provide any notice to any third party, including individuals, regulators, law enforcement agencies, or others.

c. Contractor shall be liable for damages or losses suffered by or claims against the Company relating to a Personal Information Breach resulting from Contractor's acts or omissions (including the actions and omissions of Contractor's Sub-processors). Contractor shall bear all costs associated with or resulting from (i) the investigation and resolution of the Security Breach; (ii) notifications to individuals, regulators, or others; (iii) any other remedial actions required by law, recommended by a governmental body or agreed to by the parties; (iv) provision of two (2) years of credit monitoring by a reputable provider approved by Company for affected individuals notified of a Personal

Information Breach; and (v) establishing a toll-free number and call center for affected individuals.

9. Assessments and Consultation. To the extent required by Data Protection Laws, as determined by the Company in its sole, reasonable discretion, Contractor will provide all information reasonably necessary to enable the Company to conduct and document any data protection assessments (including by performing Data Protection Impact Assessments or Data Transfer Impact Assessments if applicable) required by Data Protection Laws and engage in prior consultations with supervisory authorities, taking into account the nature of the Processing and information available to the Contractor.

10. Return or Destruction of Company Data.

a. Upon the termination or expiration of the Services for any reason, or upon Company's request at any point during the duration of this DPSA or the Agreement, Contractor will cease Processing the Personal Information and, at the choice of the Company, either return or delete and procure the return and deletion of all copies of those Personal Information within thirty (30) days. Where the Company requests the return of Personal Information, such return will be by secure file transfer in such format as is reasonably notified by the Company to Contractor.

b. Notwithstanding the foregoing, Contractor may, upon written notice to the Company and subject to the terms of this DPSA, retain Personal Information, solely to the extent and for the time period required by Data Protection Laws. Contractor will ensure that such Personal Information is only Processed as necessary for the purpose(s) specified in the law requiring its storage and for no other purpose.

c. Contractor shall provide written certification to the Company that Contractor and its Sub-processors have fully complied with this Section.

11. Audit Rights.

a. Contractor will make available to the Company all information reasonably necessary to demonstrate Contractor's compliance with its obligations under applicable Data Protection Laws. Without limitation on any audit rights set forth in the Agreement, Contractor and its Sub-processors shall permit the Company or the Company's appointed auditors to audit Contractor or its Sub-processors' compliance with this DPSA and Data Protection Laws and shall make available to the Company all copies of all information, systems, and staff reasonably necessary for the Company or its auditors to conduct such audit. After such audit, the Company will notify Contractor of any non-compliance and Contractor shall promptly take the necessary measures to remedy such non-compliance.

b. Company shall give Contractor or its Sub-processor reasonable notice of any audit or inspection to be conducted, whether by the Company or through an independent contractor, and shall take reasonable measures to minimize disruption to Contractor's or its Sub-processor's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection.

c. Contractor will provide at no cost to Company copies of any routine or other Service Organizational Control (SOC) reports, including SOC 1, Type 2, and SOC 2 reports or equivalent and other data security or data protection related audits, as applicable to the Services.

d. Contractor shall provide Company with the name and contact details of its DPO if it has appointed one or otherwise another person who is responsible for data protection compliance within Contractor.

12. Cross-Border Data Transfers of Personal Information. Contractor and Contractor's Sub-processors will not transfer any Personal Information across national borders without the prior written consent of the Company. Where the Company consents to such a transfer, Contractor will confirm a legally appropriate data transfer mechanism is in place to allow for all Restricted Transfers, including without limitation standard contractual clauses where applicable. In any event, Contractor will not transfer any Personal Information in a way that affects Contractor's protection of Personal Information, which will at all times remain at least equivalent to those security and privacy protection as required by this DPSA, the Agreement, and Data Protection Laws.

13. **No Consideration for Personal Information.** Notwithstanding anything in the Agreement or any other document, the parties acknowledge and agree that the exchange of Personal Information between the parties is not part of and is explicitly excluded from the exchange of consideration, or any other thing of value, between the parties.

14. Transfers. In the event that either party transfers to a third party Personal Information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of such party, that information shall only be used or shared consistently with applicable law.

15. Termination of This DPSA and Liability.

a. This DPSA shall terminate when the Agreement entered into between the parties is terminated and Contractor has destroyed or returned, at the Company's option, all Personal Information, and the parties' obligations under this DPSA shall survive five (5) years after the termination or expiration of the Agreement, except that Personal Data must be treated as Confidential Information in perpetuity if retained by a party.

b. Contractor shall indemnify the Company for any claims, direct or indirect costs, losses, damages, expenses (including legal expenses) and other outgoings sustained by or incurred by Contractor as a result of or arising out of Contractor's negligence or breach of this DPSA, the Company's instructions or the Data Protection Laws.

c. Notwithstanding anything to the contrary in the Agreement, the liability of Contractor under this DPSA shall not be subject to the limitations of liability provisions included in the Agreement, if any.

16. Severance. Should any provision of this DPSA be invalid or unenforceable, then the remainder of this DPSA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

EXHIBIT A

Details of Transfer

1. The categories of Data Subjects whose Personal Information is Processed or may be transferred:

[PLEASE INSERT]

2. The types of Personal Information to be Processed or that may be transferred:

The Personal Information Processed by Contractor on behalf of the Company concern the following categories of Personal Information:

[PLEASE INSERT]

3. Sensitive data transferred and applied restrictions or safeguards:

[PLEASE INSERT OR, IF NO SENSITIVE DATA IS TRANSFERRED, WRITE "N/A"]

4. Where Personal Information is transferred, the frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

[PLEASE INSERT]

5. The nature and purpose of the transfer of Personal Information and further Processing:

The nature and purpose of the Processing and, to the extent applicable, transfer, of the Personal Information are set out in the Agreement and this DPSA.

6. Duration of the Processing of Personal Information:

The Personal Information will be Processed for as long as reasonably necessary to provide the Services or to otherwise comply with Data Protection Laws.

7. The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period.

The Personal Information will be retained for as long as reasonably necessary to provide the Services or to otherwise comply with Data Protection Laws.

8. For transfers to (Sub-) processors, also specify subject matter, nature, and duration of the Processing.

[PLEASE INSERT]

EXHIBIT B

SECURITY MEASURES

Contractor

1. **Security and Privacy Governance.** Contractor maintains a cybersecurity program that documents the policies, standards, and controls it uses that secure the information and resources related to the Services. The documentation includes organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities, and the sensitivity of the Personal Information at issue.

2. **Network Management.**

   a. **Host System Configuration.** Contractor has and will configure host systems according to an industry standard, which includes but is not limited to ISO 27001. Systems must be configured to function as required and to prevent unauthorized actions.

   b. **Event Logging.** Contractor has and will log all key security-related events, including but not limited to: (1) all actions taken by any individual with root or administrative privileges; (2) access to all audit trails; (3) invalid logical access attempts; (4) use of and changes to identification and authentication mechanisms; (5) initialization, stopping, or pausing of the audit logs; and (6) creation and deletion of system-level objects.

   c. **System Network Monitoring.** Contractor has and will develop and implement a process to review log alerts and security events daily for all system components to identify anomalies or suspicious activity that include: (1) all security events; (2) logs of all critical system components; and (3) logs of all servers and system components that perform security functions. Server and system component logs must include: Firewalls; Intrusion Detection Systems (IDS); Intrusion Prevention Systems (IPS); and Authentication servers (e.g., Active Directory domain controllers). Contractor must address and document the activities taken to address all exceptions and anomalies identified during the review process.

   d. **Network Controls.** Contractor must confirm that all data and communications networks are secured to ensure the protection of Personal Information. Contractor shall: (1) disable or remove applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for any business functionality; (2) ensure that network segments connected to the Internet are protected by a firewall which is configured to secure all devices behind it; (3) network segmentation is maintained to ensure that Personal Information is isolated from non-Personal Information, logically or physically, unless approved in writing by the Company; (4) user connection capability is documented with regard to messaging, electronic mail, file transfer, interactive access, and application access; (5) all production servers are located in a secure, access-controlled location; and (6) firewalls are configured properly to address all reasonably-known security concerns. All Contractor systems must remain up to date to the current release and be actively monitored with patches promptly installed. Such monitoring must be documented and reviewed at least quarterly.

   e. **Encryption.** Contractor will encrypt all Personal Information in transit and at rest using an encryption solution that meets, at a minimum, AES-256 with 128 bit or higher encryption key.

   f. **Remote Access.** Remote access to a network containing Personal Information or access to the Company systems will be done via a secure connection (e.g., VPN). All extranet connectivity into the Company systems will be through the Company-approved and authorized secure remote connections.

   g. **Access Control.** Contractor will restrict access to Personal Information to only authorized individuals. This must be enforced accordingly to ensure that (1) only authorized individuals are permitted access to business applications, systems, networks, and computing devices containing Personal Information; and (2) user privileges are scoped to the minimum permission required to complete their assigned duties. Contractor will review user access privileges, at a minimum, every six (6) months.

   h. **Passwords and Multi-Factor Authentication.** Contractor personnel will use unique passwords that are regularly updated. All passwords must remain confidential and will not be shared between Contractor's employees, contractors, or third-party users. Contractor will implement multifactor authentication for accounts with access to Personal Information and the Company systems and networks. Contractor agrees to use multifactor authentication methods that meet industry standard criteria, as defined by NIST 800-63b.

   i. **Malware Controls.** Contractor has and will implement and manage enterprise-wide detection, prevention, and recovery controls to protect against malware that includes procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting, and recovering from malware attacks. At all times during the

provision of any Services, Contractor will make reasonable efforts to ensure that all Services do not contain malicious software or malware.

j. **Vulnerability & Threat Management.**

i. Contractor will ensure a vulnerability management program exists to eliminate vulnerabilities and threats that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes but is not limited to: (1) vulnerability remediation; (2) software and firmware patching; and (3) hardware maintenance.

ii. Contractor will ensure that all elements of a system (e.g., application software packages, system software, hardware, and services) are tested at least three (3) times, with a verifiable history of vulnerabilities being remediated after each scan before the system is promoted to a production environment. All testing must be documented, and those documents must be retained for a minimum of five (5) years unless a longer period of time is required by applicable law.

k. **Data Backups.** To ensure the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident, Contractor will ensure that backups of essential information and software, and in particular any Personal Information, are performed on a regular basis, at least every forty-eight (48) hours, according to a defined cycle in accordance with Contractor's internal policies and industry best practices. Contractor shall establish alternate and/or separate storage sites to ensure availability and accessibility of Personal Information. Contractor shall test the backup process at least quarterly.

l. **Secure Destruction.** Contractor will formally implement methods of destruction that are based on the type of media, including physical, paper-based media; physical, digital media; and electronic, digital data. Contractor will securely destroy sensitive information and maintain documentation of such destruction. Upon request, Contractor shall provide the Company (or a Company Data Subject with the Company approval) with certification of secure destruction.

m. **Virtualization & Cloud Solutions.** If Contractor utilizes a cloud solution, Contractor will adhere to the same security principles required by this Exhibit B and applicable government regulations, laws, or directives, including Data Privacy Laws, as used throughout Contractor's enterprise. The geographic location of the provider infrastructure resources must be made in writing to the Company prior to transferring any of the Company information to that provider. At all times under this Exhibit B, Contractor is required to receive prior approval of the Company, who has sole control over the data location in any cloud services to ensure compliance with local laws that restrict the cross-border flow of data.

3. **Testing.** Contractor will regularly, and in any event annually, test, assess, and evaluate, and document its compliance with this Exhibit B to ensure that the measures identified herein are effective for the security of the Processing of Personal Information.

4. **Physical Security.** Contractor will actively manage the physical security controls and ensure all buildings throughout Contractor's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) and store, process or transmit Personal Information are physically protected from unauthorized access. These physical security controls should follow security best practices, such as ISO/IEC 27002 requirements. Contractor will maintain and record facility access logs with access restricted to only those personnel with a business need. Contractor will review and update these access lists at least quarterly.

5. **Security Incident & Breach Management.** In addition to Contractors' obligations to notify of Personal Information Breaches in the Data Processing DPSA to which this Exhibit B is attached, Contractor will comply with the following obligations.

a. **Incident Management.** Contractor will document all cybersecurity incidents and maintain a documented cybersecurity event management process that covers the incident response, escalation, and remediation of cybersecurity incidents and events, including Personal Information Breaches. All such documentation must be retained for a minimum of five (5) years following the conclusion of any cybersecurity incident and event, unless otherwise required by applicable law.

Sub-processor

Contractor requires its Sub-processors to maintain security measures at least as protective as those described herein.

EXHIBIT C

SUB-PROCESSORS

[Contractor to insert:]

Name of Sub-processor	Categories of Data Processed	Affected Data Subjects	Processing Activities	Geographic Location of Data Processing

Annex 1

EU AND SWISS DATA PROTECTION OBLIGATIONS

1. **Definitions.** For purposes of this Annex:
    a. "**EU Data Protection Laws**" means the legislation of a European Economic Area country that governs the Processing of Personal Data, including the EU General Data Protection Regulation 2016/679 ("GDPR") and the laws implementing or supplementing the GDPR, the EU Directive on Privacy and Electronic Communications and the laws implementing or supplementing or superseding it, and any other applicable law with respect to any Personal Data (as that term is defined below).
    b. "**Switzerland's Data Protection Laws**" means the Federal Act on Data Protection ("FADP") of 19 June 1992, as revised as of 25 September 2020, and any other applicable law with respect to any Personal Data (as that term is defined below).
    c. "**EU Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries approved by the European Commission Decision of 4 June 2021 and available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.
    d. "**Personal Data**" means Personal Data as that term is defined by the GDPR.

2. **Requirements.** To the extent that Contractor Processes Personal Data subject to EU Data Protection Laws, Contractor shall not transfer any such data outside of the European Union or a country deemed adequate by the European Commission, without relying, for the entire duration of such transfer, on: (i) the EU Standard Contractual Clauses or subsequent standard data protection clauses adopted or approved by the European Commission as being sufficient to secure transfers of Personal Data outside of the European Union; or (ii) if agreed by the Company prior to any such transfer, an alternate mechanism in accordance with Data Protection Laws. For the purposes of the EU Standard Contractual Clauses, the following additional provisions shall apply:
    a. Company and Contractor agree to observe the terms of Module Two of the EU Standard Contractual Clauses to the exclusion of all other Modules.
    b. The competent Supervisory Authority is the EU Member State where the applicable Data Subject is located whose Personal Data is being transferred.
    c. Clause 7 "Docking Clause" is not selected by the parties.
    d. Optional Clause 11 "Redress" is not selected by the parties.
    e. Subject to the foregoing, the Company and Contractor agree to observe the terms of the EU Standard Contractual Clauses without modification.
    f. With respect to Annex I.A of the EU Standard Contractual Clauses:
        i. Company shall be regarded as the data exporter and Controller.
        ii. Contractor shall be regarded as the data importer and Processor.
        iii. The parties' signature to this DPSA shall be considered as signature to the EU Standard Contractual Clauses.
    g. The details and description of the transfer and the technical and organizational measures implemented by the importer are those specified in Exhibits A and B of the DPSA.
    h. The Sub-processors as of the Effective Date are specified in Exhibit C.
    i. The term "Member State" in the EU Standard Contractual Clauses shall not be interpreted to preclude Data Subjects in Switzerland from enforcing their rights in accordance with the EU Standard Contractual Clauses.
    j. References to the GDPR in the EU Standard Contractual Clauses shall be interpreted as references to the FADP insofar as the data transfers are subject to the FADP.
    k. The EU Standard Contractual Clauses apply to the data of legal entities until the revised FADP goes into effect.
    l. In the event of any conflict between the provisions of the EU Standard Contractual Clauses and the remaining terms of the DPSA, then the EU Standard Contractual Clauses or any replacement thereof shall take precedence. The terms of the DPSA shall not vary the EU Standard Contractual Clauses in any way.

Annex 2

UK Data Protection Obligations

1. **Definitions.** For purposes of this Annex:
   a. "**UK Data Protection Laws**" means the UK DPSA, the UK GDPR as defined by the UK DPSA as amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019, the Privacy and Electronic Communications Regulations 2003, and any other applicable law with respect to any Personal Data (as that term is defined below).
   b. "**EU Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries approved by the European Commission Decision of 4 June 2021 and available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.
   c. "**Personal Data**" means Personal Data as that term is defined by Data Protection Laws under this Annex.

2. **Requirements.** To the extent that Contractor Processes Personal Data subject to UK Data Protection Laws:
   a. Contractor shall not transfer any such data outside of the UK or a country deemed adequate by the Information Commissioner's Office (ICO), without relying, for the entire duration of such transfer, on the EU Standard Contractual Clauses as modified by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, VERSION B1.0, which is attached to this Annex as Appendix 1.

Appendix 1 to Annex 2

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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.

Part 1: Tables

Table 1: Parties

Start date	INSERT	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: INSERT Trading name (if different): INSERT Main address (if a Company registered address): INSERT Official registration number (if any) (Company number or similar identifier): INSERT	Full legal name: INSERT Trading name (if different): INSERT Main address (if a Company registered address): INSERT Official registration number (if any) (Company number or similar identifier): INSERT
Key contact	Full Name (optional): INSERT Job Title: INSERT Contact details including email: INSERT	Full Name (optional): INSERT Job Title: INSERT Contact details including email: INSERT
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorization or General Authorization)	Clause 9a (Time period)	Is Personal Data received from the Importer combined with Personal Data collected by the Exporter?
1						
2	X			Prior Authorization	Thirty (30) days	
3						
4						

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: Table 1 of this Appendix
Annex 1B: Description of Transfer: Exhibit A of the DPSA
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Exhibit B of the DPSA
Annex III: List of Sub-processors (Modules 2 and 3 only): Exhibit C of the DPSA

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 **Error! Reference source not found.**: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

This Annex incorporates by reference, and each party agrees to be bound by, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section **Error! Reference source not found.** of those Mandatory Clauses.