PERSONAL DATA PRIVACY AND PROTECTION CLAUSES FOR VENDOR CONTRACTS
(Effective December 13, 2022)

To the extent Vendor will be provided with or have access to Personal Information (as defined below), this Personal Data Privacy and Protection Clauses for Vendor Contracts (the "Addendum") is incorporated into and forms a part of the Contract by and between Vendor and Company for the purchase of goods and/or services by Company from Vendor.

1. DEFINITIONS.

1.1. "**Personal Information**" means information relating to an identified or identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

1.2. "**Data Protection Requirements**" means all applicable laws and regulations relating to the processing, protection, or privacy of Personal Information in a jurisdiction in or from which Company or Vendor collects, transmits, stores, uses, and discloses Personal Information.

1.3. "**Process**," "**Processing**," or "**Processed**" means any operation which is performed upon Personal Information, whether or not by automatic means, including but not limited to the access, acquisition, collection, recording, organization, storage, alteration, retrieval, consultation, use, disclosure, combination, "**Transfer**" (defined below), blocking**,** return or destruction of Personal Information.

1.4. "**Security Incident**" means any suspected or actual act or omission that compromises either the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place by Vendor that relate to the protection of the security, confidentiality, or integrity of Personal Information. Without limiting the foregoing, such compromise includes any unauthorized access to or disclosure or acquisition of Personal Information.

1.5. "**Transfer**" means both (a) the moving of Personal Information from one location or person to another, whether by physical or electronic means and (b) the granting of access to Personal Information by one location or person to another, whether by physical or electronic means. "**Transferred**," or "**Transferring**" will be construed accordingly.

1.6. "**EEA Covered Information**" mean European Economic Area, the United Kingdom, or Switzerland.

1.7. "**Company**" means the "Buyer", "Purchaser" or "Company" referenced in the applicable Contract that is purchasing or otherwise receiving the goods and/or services from the Vendor.

1.8. "**Vendor**" means the "Vendor", "Seller", "Supplier", "Contractor" or "Consultant" referenced in the applicable Contract that is selling or otherwise providing the goods and/or services to the Company.

2. PRIVACY AND INFORMATION SECURITY STANDARDS.

2.1. **Compliance.** Vendor will comply with the terms of this Addendum and all applicable Data Protection Requirements relating to the collection or use of Personal Information and will impose and enforce compliance with this Addendum on all its employees, sub-processors, and other third-party Vendors with access to Personal Information.

2.2. **Confidentiality.** Vendor will maintain the confidentiality of all Personal Information and will not disclose Personal Information to third parties unless the Company or the Contract specifically authorizes the disclosure, or as required by law. If a law requires Vendor to process or to disclose Personal Information, Vendor must first inform Company of the legal requirement and give Company an opportunity to object or challenge the requirement, unless the law prohibits such notice. Vendor will ensure that any persons it authorizes to process EEA Covered Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2.3. **Limitations on Use.** Vendor will process Personal Information only to the extent, and in such a manner, as is necessary for providing the Services as set out in the Contract and in accordance with Company's written instructions. Vendor will not process Personal Information for any other purpose or in a way that does not comply with this Addendum or the Data Protection Requirements.

2.4. **Limitations on Disclosure.** Vendor will not use, sell, rent, lease, transfer, distribute or otherwise disclose or share Personal Information for Vendor's own purposes or for the benefit of anyone other than Company, without Company's prior written consent.

2.5. **Sub-processors.** Vendor may only authorize a third party ("**Sub-processor**") to process Company Personal Information if Vendor enters into a written contract with the Sub-processor that contains terms substantially the same as those set out in this Privacy and Information Security Addendum.

2.6. **Security.** Vendor will adopt and implement appropriate measures, including technical and organizational safeguards, in accordance with industry standard practices and by Data Protection Requirements relating to data security.

2.7. **Notification of Security Incidents.** Vendor will provide notice to Company without undue delay after becoming aware of any Security Incident. Such notice must include details on: the incident, the Personal Information affected, the estimated number of data subjects affected, and the investigative and remedial measures undertaken or planned. Vendor has an obligation to supplement its notice with additional information that is responsive or relevant. Vendor further agrees to provide reasonable cooperation and promptly provide Company with assistance in investigating and responding to such an incident.

2.8. **Return/Deletion of Data.** On termination of the Contract for any reason or expiry of its term, Vendor will securely destroy or, if directed in writing by Company, return and not retain, the Personal Information in its

possession or control. If any law, regulation, or government, or regulatory body requires Vendor to retain any documents or materials that Vendor would otherwise be required to return or destroy, it will notify Company in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. Vendor will certify in writing that it has destroyed Personal Information within thirty (30) days after it completes the destruction.

2.9. **Audit.** Vendor will make available to Company all information necessary to demonstrate compliance with this Addendum and applicable Data Protection Requirements and allow for and contribute to audits, including inspections, by Company or an auditor mandated by Company. Vendor will make available to the auditor all information, systems, and staff necessary for the auditor to conduct such an audit. Company will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent supervisory authority; or (ii) Company reasonably believes a further audit is necessary due to a Security Incident suffered by Vendor.

3. JURISDICTION-SPECIFIC TERMS.

The following jurisdiction-specific annex applies to Vendor's processing of Personal Information:

Annex	Applicability	
	Yes	No
EEA Data Protection Compliance	☐	☐
California Consumer Privacy Act Certification	☐	☐

4. INDEMNIFICATION.

Vendor shall indemnify, keep indemnified, and defend at its own expense Company against all costs, claims, damages, or expenses incurred by Company or for which Company may become liable due to any failure by Vendor or its employees, sub-processors, or agents to comply with any of its obligations under this Addendum or applicable Data Protection Requirements.

5. NOTICE.

Any notice or other communication given to a party under or in connection with this Addendum must be in writing and delivered to:

	For Company:
Business Contact:	
Privacy Contact:	

	For Vendor:
Business Contact:	
Privacy Contact:	

6. ANNEXES.

The following Annexes are attached to, and form a part of, this Addendum:

Annex A - Details of Processing of Company Personal Data
Annex B - EEA Data Protection Compliance
Annex C - California Consumer Privacy Act Certification

7. SURVIVAL.

This Addendum survives the termination of the Contract.

8. SIGNATURES.

This Addendum has been entered into on the last date set forth below.

For Company:

Signed by [NAME OF DIRECTOR]

Signature	Date

For Vendor:

Signed by [NAME OF DIRECTOR]

Signature	Date

ANNEX A
DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex A includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

1. Subject matter and duration of the Processing of Company Personal Data:

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

2. The nature and purpose of the Processing of Company Personal Data:

[Include description here (for example, for business purpose, to comply with legal obligation, etc.)]

3. The types of Company Personal Data to be Processed:

[Include list of data types here (for example, Date of Birth, Social Service Number, any information that can be used to identify an EU Resident)]

4. The categories of Data Subject to whom the Company Personal Data relates:

[Include categories of data subjects here, (for example, Employee, Former Employee, Beneficiary, Customer, etc.)]

5. The obligations and rights of Company:

The obligations and rights of Company are set out in the Principal Agreement and this Addendum.

ANNEX B
EEA DATA PROTECTION COMPLIANCE

1. COVERED INFORMATION.
This Annex B to the Personal Data Privacy and Protection Clauses for Vendor Contracts (the "Addendum") applies to the extent that Vendor processes Personal Information collected about individuals residing in the European Economic Area, the United Kingdom, or Switzerland ("EEA Covered Information").

2. APPLICABLE LAW.
The applicable Data Protection Requirements for this Annex B include the EU General Data Protection Regulation, Regulation 2016/679, ("GDPR"); the UK GDPR, as tailored by the UK Data Protection Act 2018; and the Switzerland Federal Act on Data Protection of June 19, 1992. Capitalized terms in this Annex B that are not otherwise defined in the Addendum will have the meaning set forth in the applicable law.

3. RELATIONSHIP OF THE PARTIES.
With regard to EEA Covered Information, Company is the Data Controller and Vendor is the Data Processor.

4. LIMITATIONS ON USE.
Notwithstanding Section 2.3 of the Addendum, if applicable law requires Vendor (or, for the avoidance of doubt, any Sub-processor) to conduct processing inconsistent with any of Company's instructions, or if Vendor believes that any instruction from Company is in violation of, or would result in a violation of, applicable law, Vendor will notify Company thereof without undue delay and prior to commencing the processing.

5. GENERAL / SPECIFIC AUTHORIZATION FOR SUB-PROCESSORS.
Company provides Vendor with general authorization to engage Sub-processors to process EEA Covered Information on Vendor's behalf, provided that Vendor engages such Sub-processors in accordance with Section 2.5 of the Addendum. Upon Company's request, Vendor will provide a list of Sub-processors processing EEA Covered Information. Vendor may, by giving reasonable notice to Company, add or make changes to Sub-processors. If Company objects within thirty (30) days of such notice on reasonable grounds, then Vendor will not appoint the Sub-processor and will work in good faith with Company to find an alternative solution.

6. COOPERATION.
(a) Vendor will fully cooperate with Company in resolving any complaints, claims, or requests from individuals, including requests to access, correct, erase, or restrict EEA Covered Information; to fulfill data portability rights; or to object or withdraw consent to certain processing. If Vendor receives any such requests, it will promptly notify Company thereof, and will not respond to the request except as is necessary to confirm that the request relates to Company.
(b) If Company determines that applicable Data Protection Requirements or Company policy requires an assessment of the privacy and/or data protection impacts of any processing conducted by or on behalf of Company related to the services provided by Vendor under the Contract, Vendor will cooperate fully with and assist Company's assessment.
(c) If Company determines that applicable Data Protection Requirements or Company policy requires Company to notify, seek guidance from, or consult with any third party, including any governmental authority, competent data protection authority or representative labor body, concerning processing of EEA Covered Information for or on Company's behalf, Vendor will cooperate with Company in connection with such advisory request or consultation.

7. CROSS BORDER TRANSFERS.
Vendor will not transfer EEA Covered Information to any country or recipient not recognized as providing an adequate level of protection (within the meaning of EU Data Protection Laws), unless it first takes such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Requirements. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for EEA Covered Information, to a recipient that has achieved binding corporate rules authorization in accordance with applicable Data Protection Requirements, or to a recipient that has executed appropriate SCCs in each case as adopted or approved in accordance with applicable Data Protection Requirements. For purposes of this paragraph, "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to regulation (EU) 2016/697, as approved by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module 2 (Controller to Processor).

ANNEX C
CALIFORNIA CONSUMER PRIVACY ACT CERTIFICATION

1. COVERED INFORMATION.
This Annex C to the Personal Data Privacy and Protection Clauses for Vendor Contracts (the "Addendum") applies to the extent that Vendor processes Personal Information collected about individuals residing in the State of California ("CCPA Covered Information").

2. APPLICABLE LAW.
The applicable Data Protection Requirements for this Annex C include the California Consumer Privacy Act of 2018, as amended (codified at Cal. Civ. Code § 1798.100, *et seq.*) ("CCPA"). Capitalized terms in this section that are not otherwise defined in the Addendum will have the meaning set forth in the CCPA.

3. CERTIFICATION.
Vendor certifies (a) it is acting solely as a Service Provider with respect to the CCPA Covered Information; (b) the CCPA Covered Information it Processes is necessary to perform the services under the applicable vendor agreement(s); and (c) it complies with all applicable provisions of the CCPA and all related regulations and judicial opinions.

4. LIMITATIONS ON USE AND DISCLOSURE.
Notwithstanding Section 2.3 of the Addendum, with regard to CCPA Covered Information, Vendor possesses or controls in connection with the services provided by it to Company, Vendor will not (a) sell or "share" (as "sharing" is defined in the CCPA) such CCPA Covered Information; (b) retain, use, or disclose such CCPA Covered Information for any purpose other than the specific purpose of performing the services in the Contract, including retaining, using, or disclosing the CCPA Covered Information for a commercial purpose other than providing the services specified in the Contract; or (c) retain, use, or disclose such CCPA Covered Information outside of the direct business relationship between Vendor and Company. If Vendor can no longer meet its obligations under this Annex C or applicable law, it must notify Company and allow Company to stop and remediate any unauthorized processing.

5. COOPERATION.
Vendor will promptly cooperate with Company if an individual requests (a) access to his or her CCPA Covered Information; (b) deletion of his or her CCPA Covered Information; (c) information about the categories of sources from which the CCPA Covered Information is collected; or (d) information about the categories or specific pieces of the individual's CCPA Covered Information, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit the information to another entity without hindrance. Vendor will promptly inform Company in writing of any requests with respect to CCPA Covered Information.

6. SHARING CCPA COVERED INFORMATION WITH EMPLOYEES AND THIRD PARTIES.
Vendor will inform its employees, contractors, service providers, agents, and representatives of their CCPA compliance obligations and ensure that they comply with the CCPA and Vendor's obligations hereunder to the same extent as Vendor.