Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Terms and Conditions, Master Services Agreement, or other written or digital agreement (the "Agreement") entered into by and Customer and Company. This DPA incorporates the terms of the Agreement, and any capitalized terms that are used but not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1 "Authorized Subprocessor" means a third-party entity engaged by Company to process Personal Data in order to provide the Services and that has been approved by Customer in accordance with Section 6.

1.2 "Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account.

1.3 "Usage Data" means usage data collected and processed by Company in connection with Customer's use of the Service, including without limitation data used to identify the source and destination of a communication, activity logs, data used to optimize and maintain performance of the Service or to investigate and prevent system abuse, and data similar to any of the foregoing.

1.4 "Data Privacy Framework" means, as applicable, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework or the Swiss-U.S. Data Privacy Framework which are each administered by the U.S. Department of Commerce and any successor programs to such frameworks from time to time.

1.5 "Data Subject" means a natural person whose Personal Data is protected by Privacy Laws. For the avoidance of doubt, "Data Subject" includes the term "Consumer" under Privacy Laws.

1.6 "Data Subject Request" means a request from a Data Subject to exercise their rights over Personal Data afforded pursuant to Privacy Laws.

1.7 "EU SCCs" means standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 9 of this DPA.

1.8 "ex-EEA Transfer" means the transfer of Personal Data subject to the GDPR from the European Economic Area (the "EEA"), to a country where the transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data subject to Chapter V of the UK GDPR from outside the United Kingdom (the "UK") where such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.10 "Personal Data" means any information protected under Privacy Laws that: (i) individually or in combination, does or can identify a specific individual or by or from which a specific individual may be identified, contacted, or located; (ii) relates to an identified or identifiable natural person; an identifiable natural person 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 natural person; or (iii) is otherwise protected under Privacy Laws as "personal data", "personal information", "personally identifiable information" or using any similar or analogous terms.

1.11 "Personal Data Breach" means (i) to the extent the EU GDPR, UK GDPR or FADP is applicable, a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, or (ii) to the extent any other Privacy Laws are applicable, a confirmed security incident affecting Personal Data that Company is required to notify to Customer in accordance with such applicable Privacy Laws.

1.12 "Privacy Laws" means applicable laws, rules, or regulations relating to data privacy or data protection including, without limitation, and each to the extent applicable: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"), and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"), (ii) the Swiss Federal Act on Data Protection of 19 June 1992 as revised as of 25 September 2020 (the "FADP"), (iii) the UK Data Protection Act 2018, (iv) the EU's Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications, and the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003, (v) U.S.

state comprehensive privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "CCPA"); in each case, as updated, amended or replaced from time to time.

1.13 "Standard Contractual Clauses" means, as applicable, the EU SCCs and the UK SCCs.

1.14 "UK" means the United Kingdom of England, Wales, Scotland and Northern Ireland.

1.15 "UK Addendum" means the template International Data Transfer Addendum issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (as may be amended from time to time), as completed by Exhibit D to this DPA.

1.16 "UK SCCs" means the EU SCCs, as amended by the UK Addendum.

1.17 The terms "affiliates," "business purpose," "Controller," "Processor," "process" or "processing," "sell," "share," or "supervisory authority" shall have the meanings set forth for those or equivalent or analogous terms under Privacy Laws. For the avoidance of doubt, the terms "Controller" and "Processor" include "Business" and "Service Provider," respectively, as defined in the CCPA.

2. Role of the Parties; Description of Processing.

2.1 Except as expressly set forth in this DPA or the Agreement, with respect to Personal Data, Customer is the Controller and Company is a Processor, or to the extent Customer is a Processor to a third-party Controller, Company is a subprocessor.

2.2 Company shall process Personal Data only (i) for purposes set forth in the Agreement, (ii) in a manner consistent with the documented instructions provided by Customer, which shall include the Agreement and this DPA, and (iii) otherwise as required by Privacy Laws, other applicable laws or regulations or any competent legal or regulatory authority including any supervisory authority, in which case, Company shall inform Customer of the relevant legal requirement before processing to the extent legally permitted. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Information collected and categories of Data Subjects involved, are described in Exhibit A to this DPA.

3. Customer's Obligations. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Privacy Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Privacy Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith. Company shall immediately notify Customer if an instruction, in Company's opinion, infringes Privacy Laws or instruction of a supervisory authority.

4. Use of Personal Data. Company shall not: (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data outside of Company's direct business relationship with Customer or for any purpose other for a business purpose under the CCPA on behalf of Customer or than as necessary to perform the Services for Customer pursuant to the Agreement, except as otherwise permitted in Agreement or by Privacy Laws; and (iii) combine Personal Data received from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another party or person, except as necessary to provide the Services or as otherwise instructed by Customer or as otherwise permitted under Privacy Laws.

5. Audit.

5.1 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall make available for Customer's review copies of records demonstrating Company's compliance with prevailing data security standards applicable to the processing of Personal Data.

5.2 To the extent permitted under Privacy Laws, if Customer determines that Company is processing Personal Data in an unauthorized manner, Customer may, taking into account nature of Company's processing and the nature of the Personal Data processed by Company on behalf of Customer, and upon providing prior written notice, take commercially reasonable and appropriate steps to stop and remediate such unauthorized processing as set forth in this DPA.

5.3 If and to the extent that Privacy Laws provide Customer with a mandatory onsite inspection right, Company shall allow for onsite inspections by Customer or an independent auditor provided that: (i) Customer is able to reasonably demonstrate that the information provided by Company pursuant to Section 5.1 is insufficient for the purposes of assessing Company's compliance with Privacy Laws; (ii) the scope and timing of the inspection is mutually agreed between the parties Company in writing in advance; (iii) the inspection shall be subject to Company's applicable confidentiality controls and security policies; (iv) the inspection shall be at Customer's cost and on not less than 45 days' prior notice; and (v) Customer shall not be entitled to carry out more than one inspection in any 12 month period

5.4 If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Information), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with and subject to this Section 5. Company shall immediately notify Customer if an instruction under this Section 5, in Company's opinion, infringes Privacy Laws or the instruction of a supervisory authority.

6. Authorized Subprocessors.

6.1 Customer acknowledges and agrees that Company may (1) engage its affiliates as well as the Authorized Subprocessors listed here to this DPA to access and process Personal Data in connection with the Services (the "List") and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data pursuant to Section 6.2. By way of this DPA, Customer provides general written authorization to Company to engage subprocessors as necessary to perform the Services.

6.2 Customer acknowledges that Company may update the List from time to time. Company has provided a mechanism to subscribe to notifications of new Authorized Subprocessors (available here) and Customer agrees to subscribe to such notifications where available. At least 10 (ten) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data as a new subprocessor, Company will add such third party to the List and notify Customer. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice to Customer, provided such objection is in writing and based on reasonable grounds related to data protection. If Customer does not object during this period, the third party will be deemed an Authorized Subprocessor.

6.3 Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Company from offering the Services to Customer. If Customer reasonably objects to an engagement in accordance with Section 6.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

6.4 Company will enter into a written agreement with the Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Subprocessor fails to fulfil its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Subprocessor's obligations under such agreement.

6.5 If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Company beforehand, and that such copies will be provided by Company only upon request by Customer.

7. Confidentiality; Security of Personal Data.

7.1 Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

7.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data, as described in Exhibit C.

8. Personal Data Breach.

8.1 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such Personal Data Breach, to the extent that remediation is within Company's reasonable control.

8.2 In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Privacy Laws.

8.3 Except as otherwise required by Privacy Laws, the obligations described in Sections 8.1 and 8.2 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.1 and 8.2 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Transfers of Personal Data.

9.1 The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations may place in the United States, and that in such case the transfer of Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction that is not subject to an adequacy decision issued by the European Commission or the competent UK or Swiss authorities (as applicable), Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Privacy Laws.

9.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent that the recipient of the ex-EEA Transfer is certified accordingly, or (ii) the EU SCCs, which are deemed entered into (and incorporated herein by reference) and completed as follows:

9.2.1 Module One (Controller to Controller) of the EU SCCs applies when Company is processing Personal Data as a Controller pursuant to Section 9 of this DPA.

9.2.2 Module Two (Controller to Processor) of the EU SCCs applies when Customer is a Controller and Company is a Processor of Personal Data in accordance with Section 2 of this DPA.

9.2.3 Module Three (Processor to Subprocessor) of the EU SCCs applies when Customer is a Processor and Company is a subprocessor of Personal Data in accordance with Section 2 of this DPA.

9.3 For each module, where applicable the following applies:

9.3.1 The optional docking clause in Clause 7 does not apply.

9.3.2 In Clause 9, Option 1 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 6.1 of this DPA.

9.3.3 In Clause 11, the optional language does not apply.

9.3.4 All square brackets in Clause 13 are hereby removed.

9.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the laws of the Republic of Ireland.

9.3.6 In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.

9.3.7 Exhibit B to this DPA contains the information required in Annex I of the EU SCCs.

9.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs,

9.3.9 By entering into this DPA, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

9.4 Ex-UK Transfers. The parties agree that ex-UK Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the ex-UK Transfer is certified accordingly, or (ii) the UK SCCs, which are deemed entered into and incorporated herein by reference. The UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

9.5 Transfers from Switzerland. The parties agree that transfers of Personal Data from Switzerland to a country that is not covered by an adequacy decision from the competent Swiss authority shall either be made pursuant to (i) the Data Privacy Framework to the extent that recipient of the transfer from Switzerland is certified accordingly, or (ii) the EU SCCs with the following modifications:

9.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include FADP with respect to data transfers subject to the FADP.

9.5.2 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

9.5.3 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

9.6 Supplementary Measures. In respect of any transfer of Personal Data made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

9.6.1 As of the date of this DPA, Company has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) such Personal Data ("Government Agency Requests").

9.6.2 If Company receives a Government Agency Request, Company shall attempt to redirect the government agency to Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If Company is compelled to disclose Personal Data, to the extent legally permitted, Company shall notify Customer of the demand and reasonably cooperate to allow Customer to seek a protective order or other appropriate remedy. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. The parties shall determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light such a Government Agency Request.

9.6.3 In connection with their respective obligations under Privacy Laws to carry out a transfer impact assessments, the parties agree in good faith to confer as appropriate to consider whether: (i) the protection afforded by the laws of the relevant countries of destination provide broadly equivalent protection to that afforded in the EEA or the UK, as applicable; (ii) additional measures are reasonably necessary for any transfers to comply with Privacy Laws; and (iii) it is appropriate for Personal Information to be transferred to the relevant country, taking into account all relevant information available, including guidance by supervisory authorities, to the parties.

9.6.4 If either (i) any of the means of legitimizing a transfer cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, the Parties agree to amend the means of legitimizing transfers in accordance with Privacy Laws. In the event of any such suspension, Company shall have no liability to Customer. To the extent necessary to ensure the enforceability of the Standard Contractual Clauses, the parties shall execute the Standard Contractual Clauses as a separate agreement.

10. Data Protection Assessments. Taking into account the nature of Company's processing and the information available to Company, Company shall reasonably cooperate with Customer to conduct any data protection or privacy impact assessments as required by Privacy Laws. Notwithstanding the foregoing, Customer and Company each remain responsible only for the measures respectively allocated to them under Privacy Laws pertaining to any such assessment.

11. Data Subject Request. Company shall, to the extent permitted by Privacy Laws, notify Customer upon receipt of a Data Subject Request. If Company receives a Data Subject Request in relation to Personal Data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request. Customer is solely responsible for ensuring that that any Data Subject Requests communicated to Company are addressed in accordance with the relevant legal requirements, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject. Taking into account the nature of the processing, Company shall assist Customer through appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to Data Subject Requests.

12. Return or Destruction of Personal Data. Upon the termination or expiration of the Agreement Company shall: (i) delete the Personal Data (and all copies thereof), unless further storage of such Personal Information is required or authorized by applicable law; and (ii) at the choice of Customer, return a copy of the Personal Data to

Customer provided that Customer notifies Company of its request for a copy of the Personal Data within 10 (ten) days of termination or expiration of this Agreement. If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

13. Company's Role as a Controller. The parties acknowledge and agree that with respect to Account Data and Usage Data, Company is an independent Controller, not a joint Controller with Customer. Company will process Account Data and Usage Data as a Controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Privacy Laws. Company may also process Usage Data as a Controller to provide, optimize, and maintain the Services, to the extent permitted by Privacy Laws. Any processing by Company as a Controller shall be in accordance with Company's privacy policy.

14. Miscellaneous. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement, and (4) Company's privacy policy. Any claims brought in connection with this DPA will be subject to the Agreement, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation, limited and transient processing of Personal Data pursuant to cybersecurity vulnerability testing services.

Duration of Processing: Company will process Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Account Data and Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: The Personal Data made available to Company is determined and controlled by the Customer, in its sole discretion, while using the Services. Categories of data subject may include customer end-users, customers, and/or employees.

Categories of Personal Data: Company processes Personal Data contained in Account Data, Usage Data, and any Personal Data provided by Customer. The Personal Data made available to Company is determined and controlled by the Customer, in its sole discretion, while using the Services.

Sensitive Data or Special Categories of Data: The Personal Data made available to Company is determined and controlled by the Customer, in its sole discretion, while using the Services.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s):

Name: Customer

Address: As designated in the Agreement

Contact person's name, position and contact details: As designated in the Agreement

Signature and date: By entering into the DPA, Customer is deemed to have signed these Standard Contractual Clauses incorporated herein.

Role (controller/processor): As provided in Section 2 of this DPA.

Data importer(s):

Name: Company

Address: As designated in the Agreement

Contact person's name, position and contact details: As designated in the Agreement

Signature and date: By entering into the DPA, Company is deemed to have signed these Standard Contractual Clauses incorporated herein.

Role (controller/processor): As provided in Section 2 of this DPA.

2. Description of the Transfer

Data Subjects	As described in Exhibit A.
Categories of Personal Data	As described in Exhibit A.
Special Category Personal Data (if applicable)	As described in Exhibit A.
Nature of the Processing	As described in Exhibit A.
Purposes of Processing	As described in Exhibit A.
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A.
Frequency of the transfer	As necessary to perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA.
Recipients of Personal Data Transferred to the Data Importer	As detailed below.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

4. List of Authorized Subprocessors

https://trust.xbow.com/subprocessors

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

FRAMEWORK: The data importer has put in place a variety of technical and organizational security measures to protect Personal Data.

POLICIES: The data importer is subject to data security requirements set forth in its policies, procedures, standards and guidelines that define various aspects of required protection for Personal Data, including its written Information Security Policy.

INCIDENT MANAGEMENT: The data importer maintains documented Business Continuity, Disaster Recovery and Incident Response policies and procedures to respond to, and document responses to, relevant disruptions and events.

USER ACCESS TO INFORMATION SYSTEMS: The data importer maintains password-based, badge-based, and/or multi-factor authentication mechanisms. The data importer employs role-based access controls and grants the least privilege necessary for job function.

PHYSICAL ACCESS CONTROL: The data importer maintains role-based access controls and full-disk encryption on portable IT assets such as laptops.

IT SYSTEM SECURITY: It is the data importer's policy that business units implement various controls, processes and standards for safeguarding IT systems, which may include: controls for the prevention, detection and removal of malicious code, including malware, using approved automated and manual monitoring solutions and countermeasures; processes for identification of technical vulnerabilities and resolution where identified; minimum security requirements in network services agreements; standards for audit trails / logs that record system administrator activity, significant exceptions and information security events; processes for monitoring key systems for potentially unusual or suspicious activity and investigating exceptions; processes for the timely reporting of information security events or suspected security weaknesses and the development and execution of corrective action plans; system access controls that include user authentication, use of unique identifiers and, for remote access, two-factor authentication; and procedures to control the installation of software on operational systems.

DATA LEAKAGE/MEDIA HANDLING/CRYPTOGRAPHIC CONTROLS: The data importer employs data encryption, role-based access controls, network segmentation via firewalls, log/event monitoring, and automated 24/7 incident alerting to minimize the risk of data leakage.

THIRD PARTY SERVICE PROVIDERS: The data importer vets all third party Subprocessors to ensure that the Processing of Personal Data by such providers meets the data importer's vendor security guidelines. Subprocessors are subject to agreements governing the handling and processing of Personal Data on behalf of the data importer.

STORAGE OF PERSONAL DATA: Personal Data is to be kept only as necessary, consistent with this DPA applicable laws and regulations.

DISPOSAL OF PERSONAL DATA: When Personal Data is no longer required for business, legal or regulatory obligations, the data importer securely destroys the data.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	*See* Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of this DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	*See* Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☐ Importer ☐ Exporter ☒ Neither Party

Part 2: Mandatory Clauses

The Mandatory Clauses of the UK Addendum are incorporated herein by reference.