How to Execute this DPA:

1. Complete the information in the signature box and sign on Page 4.
2. Fill out the Exporter data in Annex I and sign on page 18.
3. Fill out Annex B: UK Addendum, Table 1 Parties.
4. Send the completed and signed DPA to privacy@loftware.com. Upon receipt of the validly completed DPA by Company at this email address, this DPA will become legally binding.

If you need additional information, please let us know at privacy@loftware.com.

Data Processing Agreement

This Data Processing Agreement ("Agreement") is made and entered into as of the date of last signature below ("Effective Date") by and between the signatory below (on behalf of itself and its affiliates hereto, hereinafter referred to as "Client", "Data Exporter" or "Controller") and Loftware, Inc. (on behalf of itself and its affiliates hereto, referred to as "Loftware," "Data Importer" or "Processor") in the execution block below (each, a "Party" and together, the "Parties"). This Data Processing Agreement is a supplement to, and made a part of, the Loftware master software and services agreement between Loftware and Client (the "Master Agreement").

1. DEFINITIONS

All capitalized terms used in this Agreement shall have the meanings given to them below:

1.1 Applicable Data Protection Law: means all applicable international, federal, national and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including, where applicable, European Data Protection Law, EEA, Switzerland Data Protection Laws and the UK GDPR).

1.2 Controller: means the entity that determines the purposes and means of the processing of Personal Data, and for the purposes of this Agreement means Client.

1.3 European Data Protection Law: means: (i) prior to 25 May 2018, the EU Data Protection Directive 95/46/EC, and any applicable national implementation of it; (ii) on and after 25 May 2018, the EU General Data Protection Regulation 2016/679 ("GDPR") and any applicable national laws made under the GDPR and (iii) 2021/914 of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council).

1.4 Personal Data: means any information relating 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.

1.5 Processor: means an entity that processes Personal Data on behalf of the Controller, and for the purposes of this Agreement means Loftware, Inc.

1.6 Standard Contractual Clauses: means Annex A attached to and forming part of this Agreement pursuant to the European Commission Decision 2021/914 of June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries.

1.7. "UK GDPR" means the aspect of the GDPR as saved into the United Kingdom by virtue of section 3 of the United Kingdom European Union (Withdrawal) Act 2018.

1.8. CCPA: means the California Consumer Privacy Act of 2018 (as may be amended from time to time).
1.9 FADP means the Swiss Ordinance to the Federal Act on Data Protection and any revisions thereto.

2. DATA PROTECTION

2.1 *Relationship of the Parties:* As between the Parties, Client is the Controller and appoints Loftware as a Processor to process the Personal Data described in Annex I of the Appendix.
2.2 *Purpose limitation:* Processor shall process the Data as a Processor only for the purposes described in Appendix 1 to Annex A, and strictly in accordance with the documented instructions of Client (the "Permitted Purpose"). In no event shall Processor (i) process the Data for its own purposes or those of any third party and (ii) not sell or share (as those terms are defined in the CCPA) Personal Data..
2.3 *International transfers of Data:* Processor will at all times provide an adequate level of protection for the Data, wherever processed, in accordance with the requirements of Applicable Data Protection Law. Processor shall not process or transfer any Data originating from the European Economic Area (EEA) in or to a territory which has not been designated by the European Commission as providing an adequate level of data protection unless (i) it has first obtained Client's prior written consent; and (ii) it executes and complies with its obligations under the Standard Contractual Clauses attached at Annex A (including its Appendices), which shall form an integral part of this Agreement. By executing this Agreement, Client understands and agrees that Processor is a company located in the United States, EU, UK, Singapore, Hong Kong, China and the Personal Data will be processed in these countries and consents to such processing. In the event of any conflict between the Standard Contractual Clauses and this Agreement, the Standard Contractual Clauses shall control and supersede.

With respect to Data transferred from the United Kingdom for which United Kingdom law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, the International data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (UK Addendum) and a document setting out transitional provisions as set in Annex B apply.

With respect to Data transferred from Switzerland for which Swiss law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

With respect to Data transferred from any European Economic Area (EEA) country for which EEA law governs the international nature of the transfer, the European Commission's standard contractual clauses (SCCs) for international data transfers, as updated from time to time, apply. References to the GDPR in Clause 4 of the SCCs shall be interpreted in accordance with the GDPR and relevant EEA data protection laws, and the concept of supervisory authority shall include the relevant EEA Data Protection Authorities.

Processor participates in the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework (together, "the Frameworks"). The parties agree that transfers of Personal Data to the United States that are subject to the Frameworks are transfers on the basis of an adequacy decision unless and until either: (i) Processor discontinues its participation with the Frameworks, or (ii) a legally binding, final decision issues that the Frameworks do not ensure an adequate level of protection under Data Protection Laws and Regulations, whichever is earlier. If the Frameworks do not apply to the transfer of Personal Data, then the Standard Contractual Clauses attached at Annex A (including its Appendices) applies.

2.4 *Confidentiality of processing:* Processor shall keep strictly confidential all Personal Data that it processes on behalf of Client. Processor shall ensure that any person that it authorises to process the Data (including Processor's staff, agents and subcontractors) (each an "Authorised Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Data who is not under such a duty of confidentiality. Processor shall ensure that only Authorised Persons will have access to, and process, the Data, and that such access and processing shall be limited to the extent strictly necessary to achieve the Permitted Purpose. Processor accepts responsibility for any breach of this Agreement caused by the act, error or omission of an Authorised Person.

2.5 *Security:* Processor shall implement appropriate technical and organisational measures to protect the Data from (i) accidental or unlawful destruction, and (ii) loss, unauthorized alteration, unauthorised disclosure of, or unauthorized access to the Data (a "Security Incident"). At a minimum, such measures shall include the security measures identified in Appendix 2 to Annex A.

2.6 *Subcontracting:* Client consents and gives general authorization to Processor engaging third party sub-Processors, to process the Data provided that: (i) Processor will provide to Client an up-to-date list of its then-current sub-Processors upon request; (ii) will enter into a written agreement with each sub-processor, imposing data protection obligations substantially similar to those set out in this Agreement; and (iii) Processor provides at least thirty (30) days' prior written notice of the addition or removal of any sub-Processor (including the categories of Data processed, details of the processing it performs or will perform, and the location of such processing). Client may reasonably object to Processor's use of a new sub-processor for reasons related to Applicable Data Protection law or other privacy or data protection related reasons by notifying Processor in writing within 15 business days after its receipt of Processor's notice of intent to use a new sub-Processor. In the event Client objects to use of a new sub-Processor, Processor will use reasonable efforts to make available to Client a change in the services. Processor's list of sub-processors will be provided in an Annex I of the Appendix to this Agreement and is maintained online at https://loftware.com/privacy. In all cases, Processor shall impose the data protection terms on any sub-Processor it appoints that at a minimum meets the requirements provided for by this Agreement and Processor shall remain fully liable for any breach of this Agreement that is caused by an act, error or omission of its sub-Processor.

2.7 *Cooperation and individuals' rights:* To the extent permitted by Applicable Law, Processor shall provide reasonable and timely assistance to Client to enable Client to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from an individual, regulator, court or other third party in connection with the processing of the Data. In the event that any

such communication is made directly to Processor, Processor shall instruct such individual to contact Client directly.

2.8 *Data Protection Impact Assessment:* If Processor believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of individuals, it shall promptly inform Client of the same. Processor shall provide Client with all such reasonable and timely assistance as Client may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

2.9 *Security incidents:* Upon becoming aware of a Security Incident, Processor shall inform Client without undue delay and shall provide such timely information and cooperation as Client may require in order for Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law and relevant contractual obligations owed by Client to its subscribers. Processor shall cooperate with Client in taking all appropriate measures and actions as are necessary to remedy or mitigate the effects of the Security Incident, shall manage and modify its systems to remedy or mitigate such Security Incident and the likelihood of future similar Security Incidents, and shall keep Client informed of all developments in connection with the Security Incident. Processor shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) Client has agreed to such notification, and/or (b) notification is required to be made by Processor under Applicable Data Protection Laws. For the avoidance of doubt, Processor shall have the right to comply with the terms of its contracts with other customers with respect to their data.

2.10 *Deletion or return of Data:* Upon termination or expiry of the Agreement, but not more than 30 days, Processor shall (at Client's request) destroy all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing); provided, however, that customer data (including Data) may be retained on backup for a period of up to thirty (30) days for legal and compliance purposes. Notwithstanding the foregoing, Processor shall not reduce the security measures at any time until such Data is permanently deleted.

2.11 *Audit:* Processor shall permit Client (or its appointed third-party auditors) to audit Processor's compliance with this Agreement, and shall make available to Client all information, systems and staff necessary for Client (or its third-party auditors) to conduct such audit. Processor acknowledges that Client (or its third-party auditors) may enter its premises for the purposes of conducting this audit, provided that Client gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Processor's operations. Client 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 data protection authority; or (ii) Client believes a further audit is necessary due to a Security Incident suffered by Processor. Processor shall also respond to any written audit questions submitted to it by Client. Notwithstanding anything else, Client understands and agrees that Processor operates a multi-tenant environment and Processor shall not be required to conduct, or permit Client or its auditors to conduct, any activities that could impair the security or confidentiality of the information of any of Processor's other customers.

2.12 *Liability:* The liability of each Party under this Agreement shall be subject to the exclusions and limitations of liability set out in the Master Agreement.

2.13 *General cooperation to remediate:* In the event that Applicable Data Protection Law, or a data protection authority or regulator, provides that the transfer or processing of Personal Data under this Agreement is no longer lawful or otherwise permitted, then the Parties shall agree to

remediate the processing (by amendment to this Agreement or otherwise) to the extent practical in order to meet the necessary standards or requirements.

2.14. *CCPA*. To the extent that the CCPA as amended applies to the Processing of Personal Data subject to this Agreement and the Master Agreement, Processor (acting as a Service Provider) will not: (i) retain, use, combine or disclose any Client's Personal Data, for any purpose other than as described in this Agreement and in the Master Agreement; or (ii) sell or share Client Personal Data to any third party. For purposes of applicable law, both parties agree that there is no sale of Personal Data involved in Processor's provision of the Services to Client. Processor certifies that it understands the restrictions set out in this Section and agrees to comply with them. For the avoidance of doubt, Client does not provide Personal Data to Processor for any monetary or other valuable consideration. For purposes of this section, all terms used but not defined shall have the meaning ascribed to them in the CCPA.

3. TERM

3.1 The obligations placed upon the Processor under this Agreement shall survive so long as Processor and/or its sub-Processors process Personal Data on behalf of Client.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized officers or representatives as of the Effective Date:

Loftware, Inc. (DATA IMPORTER):		**Client (DATA EXPORTER)**	
BY	Christopher Smith	**BY**	
NAME	Christopher Smith	**NAME**	
TITLE	General Counsel	**TITLE**	
ADDRESS	249 Corporate Drive, Portsmouth, NH 03801, USA	**ADDRESS**	
DATE	July 14, 2025	**DATE**	

ANNEX A

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Intentionally Left Blank

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be

fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another

third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

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

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

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

  (ii) the data importer is in substantial or persistent breach of these Clauses; or

  (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

  In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Slovenia.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency is able to be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): Controller

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*
Name**: Loftware, Inc.**

Address: 249 Corporate Drive, Portsmouth, NH 03801, USA

Contact person's name, position and contact details: Christopher Smith, General Counsel (privacy@loftware.com)

Activities relevant to the data transferred under these Clauses:

Data processing for the performance of the data importer's services pursuant to the agreement between data exporter and data importer.

Signature and date: Christopher Smith July 14, 2025

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees of data exporter, who are natural persons and others that are under the control of the Data Exporter and cannot be foreseen by the Data Importer.

Categories of personal data transferred

First and last name; e-mail address; title; position; employer; location data; username; password

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

Receiving data, cloud storage, allowing access, protecting data,

Purpose(s) of the data transfer and further processing
The objective of Processing of Personal Data by data importer is the performance of the data importer's services pursuant to the agreement between Client and data importer relating to the provision of services by data importer to Client.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Up to 30 days after contract termination.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The duration of the agreement between data exporter and data importer relating to the provision of services by data importer to data exporter.

Sub-processor	Country	Subject Matter	Product / Solution	Nature of Processing
Microsoft Azure	USA Country of the data centre can be chosen by customer	Cloud platform provider	Loftware Cloud (ex. NiceLabel Cloud)	User authorisation, storing data, security provisioning, web apps., databases, workflow services IT system resources provisioning, etc.

Amazon Web Services - Aws	USA Country of the data centre can be chosen by customer	Cloud platform provider	- Loftware Cloud Enterprise (ex. Spectrum) - Loftware Smartflow - Loftware Cloud Clinical Trials (ex. Prisym360) - BL.INK core - BL.INK enterprise	User authorisation, storing data, security provisioning, web apps., databases, workflow services IT system resources provisioning, etc.
Validated Cloud	USA	Cloud platform provider	Loftware Cloud Clinical Trials (ex. Prisym360)	GxP managed Platform as a Service for hosting PRISYM 360 in their data-centre in the US (Waltham, MA and San Francisco). They provision, patch, backup and monitor everything up to and including the OS and DB.
Colbright B.V.	Netherlands	Cloud platform provider	Loftware Cloud Clinical Trials (ex. Prisym360)	GxP managed Platform as a Service for hosting PRISYM 360 in their data-centre in the EU (Amsterdam and Zwolle). They provision, patch, backup and monitor everything up to and including the OS and DB. Colbright is a hosting location inside the EU.
SMTP2Go	New Zealand	Mailing cloud service	Loftware Smartflow	Smartflow application uses SMTP2Go cloud service for sending

				e-mails to their employees or customers/suppliers.
Auth0	United States	SAML SSO Identity Provider	- BL.INK core - BL.INK enterprise	Authentication, SAML
HubSpot	United States	A platform for inbound marketing, sales, and customer service.	- BL.INK core - BL.INK enterprise	Marketing, sales, and customer service platform
New Relic	United States	Network monitoring	- BL.INK core - BL.INK enterprise	Observability and Service Level Management
Nice Packaging and Labeling Products, India	India	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
Loftware, Inc., USA	USA	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
GAP Systems Ltd., UK	UK	Technical support	The entire range of Loftware products, specialised for its own Label and Artwork SaaS software solutions	Solve client problems with the Data Importer solution.
PrisymID Limited, UK	UK	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
Euro Plus d.o.o., Slovenia	Slovenia	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution

NiceLabel GmbH, Germany	Germany	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
NiceLabel Asia Pacific PTE Ltd., Singapore	Singapore	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
Loftware Asia Pacific Pte. Ltd., Singapore	Singapore	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
GAP Systems China Ltd., China	China	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution
NiceLabel Software Co. Ltd., Shanghai	China	Technical support	The entire range of Loftware products	Solve client problems with the Data Importer solution

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Informacijski pooblaščenec, Dunajska cesta 22,1000 Ljubljana, Slovenia (e-mail: gp.ip@ip-rs.si)

ANNEX II

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

The TOM shall at minimum include measures in relation to:

- Confidentiality
- Integrity
- Availability and Resilience and
- Procedures for regular testing, assessment and evaluation

The technical and organizational security measures shall be subject to change upon 120 days written notice to other entities unless the measures can be implemented immediately without extensive effort.

1. Confidentiality (Article 32 Paragraph 1 Point b of the GDPR)

1.1 Physical Access Control

Unauthorized persons are to be denied entry to the facilities in which personal data are processed or used.
Each Party has implemented the following entry control measures insofar as personal data are processed in the rooms/buildings of the company or access to such data from these rooms/buildings cannot be precluded:

1. Effective entry authorization controls through an adequate locking system, preventing infiltration by unauthorized persons, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff.
2. Limit the number of persons with access to the server room.
3. Comprehensible processes for obtaining, changing, and rescinding entry authorizations.
4. Reasonable preventive and detection measures regarding unauthorized entry and entry attempts.

1.2 Electronic Access Control

Potential use of data processing systems by unauthorized persons is to be prevented.
Each Party has implemented the following access control measures for systems and networks, in which personal data are processed or through which access to personal data is possible:

1. Effective access authorization controls through personalized and unambiguous user identification and a secure authentication process.
2. Documented and comprehensible processes for obtaining, changing, and rescinding access authorizations.
3. Restricting access authorizations to contract data to the necessary minimum.
4. Routine and documented review whether the granted access authorizations are up-to-date.
5. Reasonable measures for the protection of end-devices, servers, and other infrastructure elements against unauthorized access (e.g. secure passwords, automatic blocking/locking mechanisms two-factor authentication, encryption of data carriers/storage media, virus protection, firewall, intrusion detection systems).

1.3 Internal Access Control (permissions for user rights of access to and amendment of data)

Persons entitled to use the data processing system are only able to access personal data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied, modified or removed without authorization.

Each Party has implemented the following access control measures insofar as responsible for personal data access authorizations:

1. Restricting and logging access authorizations to personal data (need-based rights of access).
2. Separation of functionality for IT system administration and normal use.
3. Documentation of changes to access rights such as granting, changing and revoking rights.
4. Routine and documented review whether the granted access authorizations are up-to-date.

1.4 Isolation Control

Personal data collected for different purposes shall be capable of being processed separately.

1.5 Pseudonymisation (Article 32 Paragraph 1 Point a of the GDPR; Article 25 Paragraph 1 of the GDPR)

When appropriate and if so agreed taking into account the costs, scope, context and purposes and effort required by the processing of personal data shall be in such a method/way, that such data cannot be associated with a specific data subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. Integrity (Article 32 Paragraph 1 Point b of the GDPR)

2.1 Data Transfer Control

Personal data shall be incapable of being read, copied, changed, or removed during electronic transmission or during transport for storage on data carriers and there is the possibility to review and determine at what points a transmission of personal data by data transfer equipment is prescribed.
Each Party has implemented the following sharing control measures insofar as personal data shall be received, transferred, or transported:

1. Reasonable measures for securing network infrastructure.
2. Using current state-of-the-art encrypted transfer protocols classifiable as secure e.g. with Secure Socket Layer protocol (SSL), Virtual Private Networks (VPN).
3. Written rules for employees for dealing with and security of mobile devices and data carriers.

2.2 Data Entry Control

There is a possibility to subsequently review and determine whether and by whom personal data was entered into, altered in, or removed from data processing systems.
Each Party has implemented the following input control measures on its systems, which are used for processing the personal data or which enable or convey access to such systems:

1. Creation and audit-proof storage of processing protocols.
2. Securing log files against manipulation.
3. Recording and evaluating unauthorized and failed login attempts.
4. Employees do not work directly at database level, but instead use applications to access the personal data.

3. Availability and Resilience (Article 32 Paragraph 1 Point b and Point c of the GDPR)

3.1 Availability Control (Article 32 Paragraph 1 Point b of the GDPR) & Rapid Recovery (Article 32 Paragraph 1 Point c of the GDPR)

Personal Data shall be protected against accidental destruction or loss.
Each Party has implemented the following availability control measures insofar as the contract processing is required for maintaining productive services:

1. Global and redundant service infrastructure that is set up with full disaster recovery sites.
2. Creating sufficient backups.
3. Systems and data restoration processes and documentation.

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d of the GDPR; Article 25 Paragraph 1 of the GDPR)

4.1 Privacy Data Management System

4.2 Incident Response Management, including data breach

Each Party shall notify the Global DPO without undue delay after becoming aware of a personal data breach.

4.3 Contract Control and Employee control

No third-party data processing as per Article 28 GDPR is allowed without corresponding e.g.: clear and unambiguous contractual arrangements, strict controls on the selection of the processors and employees and contractors, duty of pre-evaluation, supervisory follow-up checks.
Further, all employees or contractors shall have valid permanent non - disclosure agreements in place and be educated about the importance of data protection.

4.4 Internal data privacy rules

Each Party shall have in place all regulations and processes required by the GDPR and local privacy regulation.

ANNEX B

UK ADDENDUM

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

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		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Identified in Annex I. Trading name (if different): Main address (if a company registered address): Identified in Annex I. Official registration number (if any) (company number or similar identifier): 01-0439980	Full legal name: Loftware, Inc., Trading name (if different): Main address (if a company registered address): 249 Corporate Drive, Portsmouth, NH 03801, USA Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional): Identified in Annex I. Job Title: Identified in Annex I. Contact details including email: Identified in Annex I.	Full Name (optional): Christopher Smith Job Title: General Counsel Contact details including email: privacy@loftware.com
Signature (if required for the purposes of Section 2)	Not required. The parties enter into this addendum by signing the Data Processing Agreement.	Not required. The parties enter into this addendum by signing the Data Processing Agreement.

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: June 4,2021 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 Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
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: Data exporter/processor:
Data importer/sub-processor: Loftware, Inc.

Annex 1B: Description of Transfer: Data processing for the performance of the data importer's services pursuant to the agreement between data exporter and data importer.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see Annex II of this DPA.

Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK,

	including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re- enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: 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 18 of those Mandatory Clauses.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.