E.U. DATA PROCESSING ADDENDUM
For ETQ Reliance®
(DPA VERSION DATE: July 1, 2025)

This Data Processing Addendum, including its attachments and appendices (the "**DPA**") supplements and forms part of the Master Subscription Agreement, Master Software License Agreement or other agreement between Hexagon and Customer (the "***Agreement***") governing Hexagon's services for ETQ Reliance® to Customer (the "***Services***"), and applies where, and to the extent that, Personal Data contained in the Customer Data in the ETQ Reliance® Services is Processed by Hexagon on behalf of Customer when providing Services under the Agreement. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control as it relates to the Processing of Customer's Personal Data within the scope of the DPA.

1. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

   "Controller" *and* ***"Processor"*** shall have the meaning given to those terms in the GDPR.

   "Controller to Processor Clauses" means the Standard Contractual Clauses with "Module 2" selected (which covers transfers of Personal Data from a Controller to Processor) to the extent there is an option to select a module or a module is referenced under the provisions of the Standard Contractual Clauses,

   "***EEA***" means the European Economic Area; and, for purposes of this DPA, the United Kingdom and Switzerland.

   "***EU***" means the European Union.

   "***European Data Protection Legislation***" means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein and Norway and the United Kingdom, applicable to the processing of Personal Data under the Agreement and this DPA, including: United Kingdom General Data Protection Regulation and the UK Data Protection Act 2018 (collectively "UK GDPR"); the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection (together the "Swiss FADP").

   "***GDPR***" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

   "***Hexagon Network***" means the Hexagon data center facilities, servers, networking equipment, and host software systems that are within Hexagon's control and are used to provide the Services pursuant to the Agreement.

   "***Hexagon Security Standards***" means the security standards set forth at https://www.etq.com/app/uploads/2020/08/etq-security-standards.pdf and incorporated herein by reference.

   "***Personal Data***", for purposes of this DPA, means the "personal data" (as defined in the GDPR) where such data is Customer Data and is subject to European Data Protection Legislation and processed by Hexagon for purposes of providing the Services under the Agreement.

   "***Processing***" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

   "Processor to Processor Clauses" means the Standard Contractual Clauses with "Module 3" selected (which covers transfers of Personal Data from a Processor to another Processor) to the extent there is an option to select a module or a module is referenced under the provisions of the Standard Contractual Clauses.

   "Restricted Transfer" means a transfer (directly or via onward transfer) of Personal Data Third Country outside the EEA, United Kingdom and Switzerland that is not considered to provide an "adequate level" of data protection by the European Commission, United Kingdom or Swiss authorities (as applicable).

   "Security Incident" means a breach of Hexagon's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Hexagon.

   "Standard Contractual Clauses" means the Annex to the European Commission's decision of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to third countries which do not ensure an adequate level of data protection pursuant to the GDPR.

   "Sub-processor" means another Processor engaged by Hexagon for carrying out Processing activities with respect to Personal Data.

   "Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the GDPR).

2. **Data Processing**

   a. **Compliance with Laws**. Any processing of Personal Data under the Agreement shall be performed in accordance with the applicable European Data Protection Legislation. Hexagon shall, however, not be responsible for compliance with any data protection laws or regulations applicable to Customer or Customer's industry that are not generally applicable to Processors.

   b. **Instructions for Data Processing.** Hexagon will Process Personal Data to provide the Services, in accordance with Customer's documented instructions, unless otherwise required by applicable European Data Protection Legislation to which Hexagon is subject, in which case Hexagon will notify Customer (unless that law prohibits Hexagon from doing so). Any additional or alternate instructions must be agreed between the Parties in writing, including the fees (if any) to be paid to Hexagon associated with complying with such instructions. Hexagon is not responsible for determining if Customer's instructions are compliant with applicable law; however, if Hexagon is of the opinion that a Customer's instructions infringes applicable European Data Protection Legislation, Hexagon shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction. Customer agrees that the Agreement, including this DPA, comprise Customer's complete and final instructions to Hexagon in relation to Processing of Personal Data.

   c. **Disclosure**. Hexagon will not disclose Personal Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Hexagon a demand for Personal Data, Hexagon will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Hexagon may provide Customer's contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Hexagon will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Hexagon is legally prohibited from doing so.

   d. **Deletion.** Upon expiration or termination of the Agreement, Hexagon shall delete Customer's Personal Data from Hexagon's systems in accordance with applicable law as soon as reasonably practicable, unless otherwise agreed in the Agreement or unless required by applicable law; provided, however, that Hexagon shall delete backup data and operational log data in the ordinary course of business. In the event applicable law does not permit Hexagon to delete the Personal Data, Hexagon warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination or expiration of the Agreement, except as permitted under the Agreement or required by law.

   e. **Confidentiality**. Hexagon shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

   f. **Customer Obligations.** Customer shall comply with its obligations under applicable European Data Protection Legislation in respect of its Processing of Customer Data and any Processing instructions it issues to Hexagon. Customer shall ensure all Personal Data provided to Hexagon has been collected in accordance with applicable laws and regulations and that Customer has all authorizations and/or consents necessary to provide such Personal Data to Hexagon. As between Hexagon and Customer, Customer shall have sole responsibility for the accuracy and quality of Personal Data. Customer shall keep the amount of Personal Data provided to Hexagon to the minimum necessary for the provision of the Services.

      To the extent Customer is a Processor for other controllers, Customer warrants to Hexagon that Customer's instructions and actions with respect to that Personal Data, including its appointment of Hexagon as another Processor, are lawful and have been authorized by the relevant controller(s).

3. **Security Responsibilities of Hexagon**. Hexagon shall implement and maintain the technical and organizational measures for the Hexagon Network as described in the Hexagon Security Standards, designed to help secure Personal Data against unauthorized Processing and accidental or unlawful loss, destruction, alteration, access or disclosure. Hexagon will (taking into account the nature of the Processing of Personal Data and the information available to Hexagon) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

   a. implementing and maintaining the Hexagon Security Standards in accordance with this Section 3;

   b. providing Customer with the Security Documentation in accordance with Section 5(d); and

   c. complying with the terms of Section 6 (Security Breach Notification).

      Customer acknowledges and agrees that the Hexagon Security Standards are subject to technical progress and development and Hexagon may update the Hexagon Security Standards, provided that any updates shall not materially diminish the overall security of Personal Data or the Services during Customer's subscription term.

4. **Customer's Security Responsibilities.** Customer agrees that, without prejudice to Hexagon's obligations under Section 3 (Security Responsibilities of Hexagon) and Section 6 (Security Breach Notification):

   a. Customer is solely responsible for its use of the Services, including

      i. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data;

      ii. securing the account authorization credentials, systems and devices Customer uses to access the Services; and

      iii. securing Customer's systems and devices Hexagon uses to provide the Services.

   b. Hexagon has no obligation to protect Personal Data that Customer elects to store or transfer outside of Hexagon's and its

subcontractors' systems (for example, offline or on-premises storage).

5. **Audit of Technical and Organizational Measures**.

   a. At least annually, Hexagon will undergo an audit to verify the adequacy of its security measures according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001 (the "**Audit**"). The Audit will be performed by a recognized independent third-party audit firm at Hexagon's selection and expense. Such examinations will result in the generation of an audit report ("**Report**").

   b. At Customer's written request, Hexagon will provide Customer with the last Report so that Customer can reasonably verify Hexagon's compliance with the data protection and security obligations under this DPA. The Report will constitute Hexagon's Confidential Information under the confidentiality provisions of the Agreement.

   c. In addition, to the extent required by applicable European Data Protection Legislation, including where mandated by Customer's supervisory authority, Customer, Customer's appointed auditor or Customer's supervisory authority may perform more frequent audits (including inspections). Hexagon will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit (the "**Security Documentation**"). Customer agrees to accept the Report in lieu of requesting an audit of the controls covered by the Report. The following terms apply to any audit under this Section 5(d):

      i. If a third party is to conduct the audit, Hexagon may object to the auditor if the auditor is, in Hexagon's reasonable opinion, not suitably qualified or independent, a competitor of Hexagon, or otherwise manifestly unsuitable. Such objection by Hexagon will require Customer to appoint another auditor or conduct the audit itself.

      ii. To request an audit, Customer must submit a detailed proposed audit plan to privacy@etq.com at least thirty (30) days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Hexagon will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Hexagon's security, privacy, employment or other relevant policies). Hexagon will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5(c)(ii) shall require Hexagon to breach any duties of confidentiality.

      iii. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Hexagon's health and safety or other relevant policies, and may not unreasonably interfere with Hexagon business activities.

      iv. Customer will promptly notify Hexagon of any non-compliance discovered during the course of an audit and provide Hexagon any audit reports generated in connection with any audit under this Section 5(c), unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of the parties under the terms of the Agreement.

      v. Any audits, other than the Audit, are at Customer's expense. Customer shall reimburse Hexagon for any time expended by Hexagon or its Sub-processors in connection with any audits or inspections under this Section 5(c) at Hexagon's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

   d. If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing Hexagon to execute the audit as described in Section 5(c) of the DPA. Requests by Customer to conduct an audit under this DPA shall be limited to once per calendar year unless (i) such audit is deemed mandatory under Section 5(c), or (ii) Customer requests an audit on the basis that there are indications of Hexagon's non-compliance with this DPA or European Data Protection Legislation and Customer has provided evidence to Hexagon of reasonable identified indications of non-compliance.

   e. Customer is solely responsible for reviewing the information made available by Hexagon relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

6. **Security Breach Notification**.

   a. If Hexagon becomes aware of any Security Incident, Hexagon will (a) notify Customer of the Security Incident without undue delay and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

   b. Customer agrees that:

      i. An unsuccessful attempt is not a Security Incident and will not be subject to this Section. An unsuccessful attempt is one that results in no unauthorized access to Personal Data or to any of Hexagon's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents;

      ii. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident(s); and

iii. Hexagon's obligation to report or respond to a Security Incident under this Section 6 is not and will not be construed as an acknowledgement by Hexagon of any fault or liability of Hexagon with respect to the Security Incident.

c. Notification(s) of Security Incidents, if any, will be delivered to Customer in accordance with the requirements for notices set forth in the Agreement.

7. **Sub-processing.**

a. **Authorized Sub-processors**. Customer agrees that Hexagon and Hexagon Affiliates may use Sub-processors to fulfill its contractual obligations under this DPA or to provide certain Services on its behalf, provided such use complies with the subcontracting provisions of the Agreement. Customer specifically authorizes the engagement of Hexagon's Affiliates as Sub-processors, and Customer generally authorizes the engagement of the Sub-processors included on the Sub-processor list provided by Hexagon and made available at: https://www.etq.com/legal-agreements/etq-sub-processors/. Except as set forth in this Section 7, or as Customer may otherwise authorize, Hexagon will not permit any subcontractor to access Personal Data.

b. **Sub-processor Obligations**. Where Hexagon engages any Sub-processors as described in this Section 7:

i. Hexagon will restrict the Sub-processors' access to Personal Data only to what is necessary to maintain the Service or to provide the Service to Customer in accordance with the Agreement and this DPA, and Hexagon will prohibit the Sub-processor from accessing Personal Data for any other purpose;

ii. Hexagon will impose appropriate contractual obligations in writing upon the Sub-processor that are no less protective than this DPA, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

iii. Hexagon will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors.

c. **Opportunity to Object to Sub-processor Changes**. When any new Sub-processor (which shall not include Affiliates) is engaged during the term of this DPA, Hexagon will, at least 30 days before the new Sub-processor Processes any Personal Data, notify Customer of the engagement (including the name and general location of the relevant subcontractor and the activities it will perform). Customer may legitimately object to any new Sub-processor by providing written notice to Hexagon within ten (10) business days of being informed of the engagement of the Sub-processor. Legitimate objections must contain reasonable and documented grounds relating to a Sub-processor's non-compliance with applicable European Data Protection Laws. In the event Customer objects to a new Sub-processor, Customer and Hexagon will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Hexagon.

d. **Access to Sub-process agreements**. Where copies of any Sub-processor agreements must be provided pursuant to the Standard Contractual Clauses described in Section 11 (Data Transfers), the parties agree said agreements may have all commercial information or clauses unrelated to the Standard Contractual Clauses or their equivalent removed by Hexagon beforehand; and that such copies will be provided by Hexagon in a manner to be determined in its discretion, only upon written request by the Customer.

8. **Impact Assessments and Consultations**. Hexagon will (taking into account the nature of the Processing and the information available to Hexagon) reasonably assist Customer in complying with its obligations under European Data Protection Legislation in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. making available for review copies of the Reports or other documentation describing relevant aspects of Hexagon's information security program and the security measures applied in connection therewith; and

b. providing the information contained in the Agreement including this DPA.

9. **Data Subject Rights**.

a. **Customer's Responsibility for Requests**. During the term of this DPA, if Hexagon receives any request from a data subject in relation to Personal Data, Hexagon will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request.

b. **Data Subject Request Assistance**. Hexagon will (taking into account the nature of the Processing of Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in in Chapter III of the GDPR. Customer shall reimburse Hexagon for any such assistance beyond providing self-service features included as part of the Services at Hexagon's then-current professional services rates, which shall be made available to Customer upon request.

10. **Processing Records.** Customer acknowledges that Hexagon is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which Hexagon is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the Processing of Personal Data,

Customer will, where requested, provide such information to Hexagon, and will ensure that all information provided is kept accurate and up-to-date.

11. **Data Transfers.** Customer understands that Hexagon is part of a global enterprise, and that Hexagon may store and Process Personal Data anywhere Hexagon or its Affiliates or subcontractors maintain facilities.

    a. **Modules.** Where Customer is a Controller of Personal Data under this DPA, the Controller to Processor Standard Contractual Clauses shall apply. Where Customer is a Processor of Personal Data under this DPA, the Processor to Processor Standard Contractual Clauses shall apply.

    b. **Customer's Transfer Obligations.** With respect to transfer of Personal Data, Customer agrees that if under European Data Protection Legislation Hexagon reasonably requires Customer to enter into Standard Contractual Clauses or use another appropriate safeguard offered by Hexagon, and Hexagon reasonably requests that Customer take any action (which may include execution of documents) required to give full effect to such solution, Customer will do so.

    c. **Restricted Transfers (GDPR).** Subject to the deviations set forth in Sections 11(d) and 11(e) below, where and to the extent that the transfer of Personal Data to Hexagon is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses (including its Annexes) in accordance with Commission Implementing Decision (EU) 2021/914 of June 4, 2021, and the Standard Contractual Clauses attached hereto as Attachment I (including its Annexes), shall be deemed incorporated into and form an integral part of the DPA.

    d. **Restricted Transfers (UK GDPR)**. Where the transfer of Personal Data to Hexagon is a Restricted Transfer of Personal Data protected by the UK GDPR, the Standard Contractual Clauses shall be deemed amended and interpreted in accordance with Part 2 of the UK Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum"), and the UK Addendum attached hereto as Schedule A (in addition to the Standard Contractual Clauses (including its Annexes) in Annex II hereto) shall be deemed incorporated into and form an integral part of the DPA.

    e. **Restricted Transfers (Swiss FADP).** Where the transfer of Personal Data to Hexagon is a Restricted Transfer of Personal Data protected by the Swiss FADP, the Standard Contract Clauses shall be deemed amended and interpreted in accordance with the Swiss Addendum to the EU Commission Standard Contractual Clauses ("Swiss Addendum"), and the Swiss Addendum attached hereto as Schedule B (in addition to the Standard Contractual Clauses (including its Annexes) in Annex II hereto) shall be deemed incorporated into and form an integral part of the DPA.

12. **Duties to Inform**. Where Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being Processed by Hexagon, Hexagon will inform Customer without undue delay. Hexagon will, without undue delay, notify all relevant parties in such action (e.g., creditors, bankruptcy trustee) that any Personal Data subjected to those proceedings is Customer's property and area of responsibility and that Personal Data is at Customer's sole disposition.

13. **Notices.** Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Hexagon to Customer may be given (a) in accordance with the notice clause of the Agreement; (b) to Hexagon's primary points of contact with Customer; and/or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

14. **Limitation of Liability.**

    a. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Hexagon, and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to all Security Incidents and any breach of the DPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) shall remain subject to the "Limited Liability" Section of the Agreement, and any reference in such Section to the liability of Hexagon means the aggregate liability of Hexagon and all of its Affiliates under the Agreement and the DPA.

    b. Where a Security Incident and/or breach of the DPA is also a breach of any confidentiality or nondisclosure obligations in the Agreement, the liability cap in Section 14.1 of the DPA will apply.

    c. Nothing in the DPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities which cannot be limited under mandatory applicable law. No one other than a Party to the DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

15. **General.** This DPA was last updated on the DPA Version Date set forth above and is made effective between the Parties as of the date Customer enters into the Agreement, or the above DPA Version Date if the Agreement was effective prior to the publishing of this version of the DPA and Services are ongoing under the Agreement as of the DPA Version Date. This DPA shall replace and supersede any existing data processing addendum that the Parties may have previously entered into regarding the Processing of Customer Personal Data in connection with the Services under the Agreement. Notwithstanding any expiration or termination of the Agreement, the DPA, including its attachments, will remain in effect until, and automatically expire upon, Hexagon's deletion of all Personal Data as described in the DPA. Hexagon reserves the right to revise the terms of the DPA at any time by posting a revised version on https://www.etq.com/app/uploads/2020/08/etq-data-processing-addendum.pdf (or any supplemental or successor web pages). Except as amended by this DPA, the Agreement will remain in full force and effect.

Annex 1
Subject Matter and Details of the Data Processing

Subject Matter	Hexagon's provision of the Services to Customer.
Duration of the Processing	Until deletion of all Customer Personal Data by Hexagon in accordance with the DPA.
Nature and Purpose of the Processing	Hexagon will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the DPA. Processing operations include storage on Hexagon's network, analysis, facilitating the Customer's use of the Hexagon software and related services and support.
Categories of Data	Data relating to individuals provided to Hexagon in connection with the Services, by (or at the direction of) Customer. Customer determines what Personal Data it provides to Hexagon.
Data Subjects	Data subjects include the individuals about whom Hexagon Processes data in connection with the Services. For example, Customers' clients.
Data Protection Contact Points – Customer (Data Exporter)	Contact Person Name: Contact Person Position: Contact Person Contact Details: Data Protection Officer (DPO) Name: DPO Contact Details: EU Representative Name: EU Representative Contact Details: [UK Representative Name:] [UK Representative Contact Details:]
Data Protection Contact Points –(Data Importer)	Contact Person Name: Tracey Fogerty Contact Person Position: General Counsel Contact Person Contact Details: tracey.fogerty@hexagon.com Data Protection Officer (DPO) Name: N/A DPO Contact Details: N/A EU Representative Name: N/A EU Representative Contact Details: N/A [UK Representative Name:] N/A [UK Representative Contact Details] N/A

Annex 2

STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR AND PROCESSOR TO PROCESSOR)

The parties agree to that with respect to the implementation of the Standard Contractual Clauses under the DPA, either one or both of Module Two: Controller to Processor of the Standard Contractual Clauses ("**Module Two**") and Module Three: Processor to Processor of the Standard Contractual Clauses ("**Module Three**") shall apply, and both Module Two and Module Three are referenced herein. To the extent Module Two and Module Three differ, those differences are highlighted below. Where Module Two and Module Three do not differ, the identical provisions are referenced only once.

As specified in the Standard Contractual Clauses below, for both Module Two and Module Three, the following optional selections are made:

1. Clause 7: Docking Clause has been selected
2. Clause 9(a) Use of Sub-processors: Option 2 - General Written Authorization, with a time period to inform of "at least thirty (30) days in advance" has been selected.
3. Clause 11 Redress: The option to lodge complaints to an independent dispute resolution body shall not apply.
4. Clause 17 Governing Law: Option 1 has been selected and the governing law for the purposes of Clause 17 shall be the Republic of Ireland.
5. Clause 18(b) Choice of Forum and Jurisdiction: The courts under Clause 18(b) shall be the court of the Republic of Ireland.

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 and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal 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 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) **For Module Two:** Clause 8.1(b), 8.9(a), (c), (d) and (e); For **Module Three**: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) **For Module Two:** Clause 9(a), (c), (d) and (e); For **Module Three:** 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

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I. A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

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 the 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 (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, 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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

(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 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. 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 , 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 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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

FOR MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR

(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.

FOR MODULE THREE: TRANSFER PROCESSOR TO PROCESSOR

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

(a) 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.

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

(c) 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) Where the data exporter is established in an EU Member State: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I. C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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;

(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 transferred personal data 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the Republic of Ireland.

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 the Republic of Ireland.

(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.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):

The entity identified as "Customer" in the DPA is the data exporter acting as controller and processor (as described in Section 2(a) of the DPA).

Details of contact person, data protection officer and/or representative (as applicable) are set out in in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

Data importer(s):

Intergraph Corporation, Hexagon's Asset Lifecycle Intelligence division (a provider of quality and compliance management software) is the data Importer acting as processor or (sub) processor (as described in Section 2(a) of the DPA).

Details of contact person, data protection officer and/or representative (as applicable) are set out in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The data subjects concerned as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

Categories of personal data transferred:

The categories concerned as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

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:

The special categories of data as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

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

Continuous.

Nature of the processing:

The nature of the processing as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

Purpose(s) of the data transfer and further processing:

The purpose of the processing as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

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

The duration of the processing as identified in Annex 1 of the DPA (Subject Matter and Details of the Data Processing).

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

As identified in the Sub-Processor list referenced in Section 7(a) of the DPA above as appropriate.

C. COMPETENT SUPERVISORY AUTHORITY

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

Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the EU Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority shall be the supervisory authority in the Republic of Ireland, namely the Data Protection Commission (DPC) (https://www.dataprotection.ie).

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

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

Hexagon maintains a list of its security standards at: https://www.etq.com/app/uploads/2020/08/etq-security-standards.pdf.

As stated in 7(b) (Obligations of Sub-processors) of this DPA, Hexagon will impose appropriate contractual obligations on its Sub-processors that are no less protective than this DPA, including relevant contractual obligations regarding confidentiality and data security.

Annex III
List of Authorized Sub-processors

Hexagon maintains a list of its sub-processors at: https://www.etq.com/legal-agreements/etq-sub-processors/

SCHEDULE A

a. INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

Background

(B) 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.

a. AGREED TERMS

PART 1: TABLES

i. TABLE 1: PARTIES

Start date	Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As described in Annex 1 to the Standard Contractual Clauses.	As described in Annex 1 to the Standard Contractual Clauses.
Key Contact	As described in Annex 1 to the Standard Contractual Clauses.	As described in Annex 1 to the Standard Contractual Clauses.

ii. TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): The EU Standard Contractual Clauses (Module 2) attached to this Agreement to which this Addendum is Annexed. Other identifier (if any): N/A Or

iii. 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: See Annex 1 of the Standard Contractual Clauses.

Annex 1B: Description of Transfer: Processing operations include storage on importers network, analysis, facilitating Exporter's use of the Services and related Professional Services and support.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 1 C of the Standard Contractual Clauses.

Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III of the Standard Contractual Clauses

iv. 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 0: ☐ ~~Importer~~ ☐ ~~Exporter~~ ☒ Neither Party

b. PART 2: MANDATORY CLAUSES

i. Entering Into This Addendum

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.

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.

ii. Interpretation of this Addendum

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 0.
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.

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.

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.

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

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.

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.

iii. Hierarchy

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 0 will prevail.

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.

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.

iv. Incorporation of and changes to the EU SCCs

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 0 to 0 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.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) 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.

v. Amendments to this Addendum

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.

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.

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.

If the ICO issues a revised Approved Addendum under Section 0, 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.

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.

Schedule B

Swiss Addendum to the EU Commission Standard Contractual Clauses

The Swiss Addendum amends the EU Standard Contractual Clauses as set out in Attachment I above to align with the Swiss FADP, following the FDPIC's guidance "The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts" that was published on 27 August 2021.

Amendments to Attachment I are as follows:

Attachment I Reference	**Swiss Addendum**	
	Case 1: **Data transfer is exclusively subject to the FADP**	**Case 2:** **The data transfer is subject to both the FADP and the GDPR.** The parties adopt the GDPR standard for all data transfers.
Competent supervisory authority in Annex I.C under Clause 13	FDPIC is the supervisory authority under Clause 13 and this overwrites the authority as recorded in Annex I.C of the Part 1**:** Office of the Federal Data Protection and Information Commissioner (FDPIC) Feldeggweg 1 CH - 3003 Berne Telefon: +41 (0)58 462 43 95 Telefax: +41 (0)58 465 99 96	**Parallel supervision:** Insofar as the data transfer is subject to the FADP the FDPIC is the supervisory authority under Clause 13; Insofar as the data transfer is subject to the GDPR the authority as recorded in Annex I.C of the Attachment I is the supervisory authority under Clause 13.
Applicable law for contractual claims under Clause 17	Swiss law	As recorded in Annex 2 – no changes
Place of jurisdiction for actions between the parties pursuant to Clause 18(b)	Swiss courts with jurisdiction in the data exporter's place of business	As recorded in Annex 2 – no changes
Place of jurisdiction for actions brought by data subjects pursuant to Clause 18(c)	The term 'member state' as used in Clause 18(c) must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland).	
Adjustments or additions regarding references to the GDPR	All references to the GDPR in Annex 2 are to be understood as references to the FADP, as applicable.	As recorded in Annex 2 – no changes