DATA PROTECTION ADDENDUM

This Data Protection Addendum (the "**DPA**") is entered into by and between PerkinElmer Informatics, Inc. ("**PerkinElmer**" or the "**data importer**"), having an address at 940 Winter Street, Waltham, MA 02451 and Customer (as defined in the Agreement) and is effective as of the start date of the Service subscription term.

WHEREAS, Customer has purchased from PerkinElmer licenses to access and use its software-as-a-service offerings as identified in the applicable Quote (the "**Service(s)**"); and

WHEREAS, in the process of providing the Service to Customer, PerkinElmer may act as a data processor of certain personal data that is entered into or uploaded into the Service by Customer and its Users; and

WHEREAS, the parties intend to ensure compliance with Data Protection Laws (as defined below) by entering into this DPA if such is required under any Data Protection Laws; and

WHEREAS, pursuant to Clause 2(a) of the SCC (as defined below), the parties may agree to add to or supplement the terms of the SCC, provided that such additional or supplemental terms do not contradict the SCC; and

WHEREAS, the parties agree to be bound by this DPA and, if and as applicable, the SCC and/or the UK Addendum, as added to and supplemented by the terms and conditions set forth herein.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereby agree as follows:

1. Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

   1.1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with the applicable party hereto, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

   1.1.2 "**Agreement**" means the software-as-a-service license agreement entered by the parties for the provision of the Service;

   1.1.3 "**Customer Group Member**" means Customer or any Customer Affiliate;

   1.1.4 "**Customer Personal Data**" means any Personal Data Processed by a PerkinElmer Processor on behalf of a Customer Group Member pursuant to or in connection with the provision of the Service;

   1.1.5 "**Data Protection Laws**" means, solely if and to the extent applicable to the Processing carried out pursuant to the Agreement, (a) GDPR; (b) the UK Data Protection Act 2018, including the UK GDPR (as defined in Exhibit B); (c) the Swiss Federal Data Protection Act; (c) the California Consumer Privacy Act ("**CCPA**"); and (d) any other data protection or privacy laws of any other country applicable to Customer Group Members or Customer Personal Data;

1.1.6 "**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;

1.1.7 "**PerkinElmer Processor**" means PerkinElmer or any PerkinElmer Subprocessor;

1.1.8 "**Restricted Transfer**" means a transfer of Customer Personal Data from any Customer Group Member to a PerkinElmer Processor, or an onward transfer of Customer Personal Data from a PerkinElmer Processor to a PerkinElmer Processor, or between two establishments of a PerkinElmer Processor, and in each case, where such transfer would be prohibited by Data Protection Laws in the absence of an adequacy mechanism ensuring the protection of personal data to be established pursuant to this DPA;

1.1.9 "**SCC**" or "**EU SCC**" means the Standard Contractual Clauses implemented by the European Commission pursuant to the Commission Implementing Decision (EU) 2021/914 of June 4, 2021, attached hereto as Exhibit A;

1.1.10 "**Swiss Standard Contractual Clauses**" means the SCC, as attached hereto, and amended to replace any references: (i) to GDPR or any predecessor regulations relating to the protection of personal data with references to the Swiss Federal Data Protection Act, (ii) to the laws of the EU or Member States with reference to the laws of Switzerland, and (iii) competent supervisory authorities or competent courts with references to the data protection authorities and courts of Switzerland;

1.1.11 "**Subprocessor**" means any entity (including any third party entity and any PerkinElmer Affiliate, but excluding an employee of PerkinElmer or any of its sub-contractors) appointed by or on behalf of PerkinElmer or any PerkinElmer Affiliate to Process Customer Personal Data on behalf of any Customer Group Member in connection with the Agreement.

1.1.12 "**UK Addendum"** means the international data transfer addendum to the SCC for international data transfers as promulgated by the Information Commissioner's Office, effective as of March 21, 2022, attached hereto as Exhibit B.

The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing," "Supervisory Authority," shall have the same meaning as the term or similar terms for the same subject matter, as set forth in the Data Protection Laws, and their cognate terms shall be construed accordingly.

The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

Capitalized terms not otherwise defined in this Section 1 shall have the meaning given to them in the Agreement.

2. Authority. PerkinElmer warrants and represents that, before any PerkinElmer Affiliate Processes any Customer Personal Data on behalf of any Customer Group Member, PerkinElmer's entry into this DPA as agent for and on behalf of that PerkinElmer Affiliate will have been duly and effectively authorized (or subsequently ratified) by that PerkinElmer Affiliate.

3. Processing of Customer Personal Data. PerkinElmer shall: (a) comply with all Data Protection Laws in the Processing of Customer Personal Data; (b) not Process Customer Personal Data other than (i) on the relevant Customer Group Member's documented instructions (with all processing as required to provide the Service and associated professional and support services deemed to constitute Customer's documented instructions pursuant to this clause); (ii) to provide the Services to the relevant Customer Group Member; (iii) to provide such other processing as set forth in the Agreement; or (iv) as required by the applicable laws of any country having competent jurisdiction over PerkinElmer or the Customer Personal Data being processed, and in the event of processing under this subsection (iv), PerkinElmer or the relevant PerkinElmer Affiliate shall, to the extent permitted by applicable law, inform the relevant Customer Group Member of such legal requirement before commencing such Processing; (c) not sell Customer Personal Data; and (d) promptly inform the relevant Customer Group Member if, in its reasonable opinion, any Customer Group Member's instructions hereunder violates any Data Protection Law.

4. PerkinElmer Personnel. PerkinElmer shall take reasonable steps to ensure the reliability of any employee, agent or contractor ("**PerkinElmer Representatives**") of any PerkinElmer Processor who may have access to Customer Personal Data, ensuring in each case (a) that such PerkinElmer Representatives are aware of the confidential nature of the Customer Personal Data, PerkinElmer's confidentiality obligations, and the obligations of Data Protection Laws; (b) that access is strictly limited to those individuals who need to know or access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement; and (c) ensuring that all such individuals are subject to binding, legally enforceable confidentiality and non-use obligations at least as stringent as those set forth herein.

5. Security. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, PerkinElmer shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected. In assessing the appropriate level of security, PerkinElmer shall take account of the particular risks presented by the Processing to be undertaken, including risks associated with a Personal Data Breach.

6. Subprocessing. Customer agrees that PerkinElmer's sub-processors are listed at: https://informatics-support.perkinelmer.com/hc/en-us/sections/4407060712212-Legal-Resources, and PerkinElmer will notify Customer of the intended engagement of any new or changed sub-processors once Customer has subscribed to follow the foregoing page. Customer shall be deemed to have consented to the use of such sub-processor unless Customer provides notice to PerkinElmer of its objection within thirty (30) days of the date of notice of such intended change. If Customer objects to the use of such sub-processor, PerkinElmer shall provide all reasonable documentation in its possession to assure Customer that the proposed sub-processor adheres to security and privacy terms substantially similar to those set forth herein and, in applicable, of the SCC. Following the provision of such information, if Customer continues to object to the use by PerkinElmer of such sub-processor, Customer's sole and exclusive remedy shall be to terminate its subscription to the Service, and PerkinElmer shall provide to Customer a refund of any prepaid fees for the Service for the period remaining following the date of termination. With respect to each Subprocessor, PerkinElmer shall: (a) carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Agreement and this DPA and, if applicable, the

SCC; (b) ensure that Subprocessor's Processing of Customer Personal Data is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA and complies with Data Protection Laws; and (c) remain responsible and liable for the acts and omissions of each Subprocessor to the same extent as if PerkinElmer performed such act or omission. PerkinElmer will provide to Customer for review such copies of the PerkinElmer Processor's agreements with Subprocessors (which may be redacted to remove confidential information not relevant to the requirements of this DPA) as Customer may request from time to time (but no more than once per calendar year).

7. Data Subject Rights. Taking into account the nature of the Processing, PerkinElmer shall assist each Customer Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer Group Members' obligations to respond to requests by Data Subjects to exercise its rights under Data Protection Laws. PerkinElmer shall: (a) promptly notify Customer if any PerkinElmer Processor receives a request from a Data Subject to exercise its rights under any Data Protection Law in respect of Customer Personal Data; (b) reasonably cooperate with any Customer Group Member in responding to such request; and (c) ensure that neither it nor the PerkinElmer Processor responds to that request except (i) for automated emails acknowledging receipt, and (ii) on the documented instructions of Customer or the relevant Customer Affiliate or as required by Data Protection Laws to which the PerkinElmer Processor is subject, in which case PerkinElmer shall to the extent permitted by applicable law inform Customer of that legal requirement before the PerkinElmer Processor responds to the request.

8. Personal Data Breach. PerkinElmer shall notify Customer without undue delay, and in any event within seventy-two (72) hours, upon PerkinElmer or any PerkinElmer Processor becoming aware of a Personal Data Breach affecting Customer Personal Data. PerkinElmer will provide Customer with such information in its possession to allow each Customer Group Member to meet any reporting and notice obligations regarding such Personal Data Breach pursuant to Data Protection Laws. Such notification shall, at a minimum:

- describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Customer Personal Data records concerned;
- communicate the name and contact details of PerkinElmer's data protection officer or other relevant contact from whom more information may be obtained;
- describe the likely consequences of the Personal Data Breach; and
- describe the measures taken or proposed to be taken to address the Personal Data Breach.

PerkinElmer shall provide prompt updates to Customer as more information regarding the Personal Data Breach becomes available. PerkinElmer shall reasonably co-operate with each Customer Group Member and take such reasonable commercial steps as are requested by Customer to assist Customer and its appointed representatives in the investigation, mitigation, remediation of, and any other response deemed appropriate by Customer to, each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation. PerkinElmer shall provide, at Customer's sole cost and expense, reasonable assistance to each Customer Group Member with such Customer Group Member's performance of data protection impact assessments, and shall provide reasonable assistance with consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the PerkinElmer Processors.

10. Deletion or Return of Customer Personal Data. (a) Subject to Section 10(b) and the terms of the Agreement, and following Customer Group Member's request made within twenty (20) days following the expiration or termination of the subscription term for the Services, PerkinElmer shall promptly provide to the relevant Customer Group Member the Customer Personal Data uploaded and entered into the Service, and shall destroy or delete such Customer Personal Data in accordance with its internal policies for deleting Service tenants. (b) Each PerkinElmer Processor may retain Customer Personal Data to the extent required by Data Protection Laws or other applicable law, but only to the extent and for such period as required by such law, and always provided further that each PerkinElmer Processor shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

11. Audit rights. No more than once per calendar year, PerkinElmer shall allow for and contribute to audits by a Customer Group Member solely by making available such information as is reasonably necessary to demonstrate compliance with this DPA and Data Protection Laws. The parties agree that the audits to be carried out hereunder or permitted to be conducted pursuant to the SCC shall be carried out in accordance with the following specifications: Upon Customer Group Member request, and subject to the confidentiality obligations set forth in the Agreement, PerkinElmer and/or the applicable PerkinElmer Affiliate shall make available to Customer (or Customer's independent, third-party auditor reasonably acceptable to PerkinElmer and that has signed a confidentiality agreement) information regarding PerkinElmer's compliance with the obligations set forth in this DPA in the form of a SOC 1/SOC 2 report in accordance with SSAE 18 or an ISO certification relevant for the Processing. Before the commencement of any audit requiring PerkinElmer's production of other documentation or other information reasonably sufficient to evidence its technical, organizational and administrative measures relevant to the Processing performed under the Agreement, Customer Group Member and PerkinElmer shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify PerkinElmer with information regarding any non-compliance discovered during the course of an audit.

Notwithstanding anything in the Agreement or the SCC, the parties hereby agree that any audit rights granted by any PerkinElmer sub-processor under Clause 8.9 and 9(b) of the SCC shall be exercisable by Customer solely by PerkinElmer's provision to Customer of any industry standard certifications, reports or attestations ("**Reports**") held by such sub-processor (with any confidential information of the applicable party redacted), or, in the absence of such Reports, by providing to Customer assessments, reports or other documentation of PerkinElmer's or sub-processors' security and privacy controls, as applicable (together with the Reports, the "**Assessments**"). The provision of all such Assessments shall be subject to and governed by the confidentiality and non-use obligations of the Agreement.

12. Restricted Transfers. Solely if and as required to enable any Restricted Transfer under Data Protection Laws, and in the event there is no other adequacy mechanism in place, the parties hereby agree to enter into, and be bound by:

- For Restricted Transfers from the EEA, the SCC;
- For Restricted Transfers from the UK, the UK Addendum; and
- For Restricted Transfers from Switzerland, the Swiss Standard Contractual Clauses.

The SCC, UK Addendum or Swiss Standard Contractual Clauses shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of Data Protection Law.

13. Limit of Liability. The parties hereby agree that, if the SCC, UK Addendum or Swiss Contractual Clauses apply, Clause 12(a) of the SCC shall apply to damages sustained by data subjects only, and, as between the parties, the limit of liability clauses of the Agreement shall apply.

14. Order of precedence. Nothing in this DPA reduces PerkinElmer's or any PerkinElmer Affiliate's obligations under the Agreement in relation to the protection of Customer Personal Data or permits PerkinElmer or any PerkinElmer Affiliate to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the SCC (or UK Addendum or Swiss Contractual Clauses), the SCC (or UK Addendum or Swiss Contractual Clauses) shall prevail. In the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail solely in regards to the protection of Customer Personal Data.

15. Changes in Data Protection Laws. The parties shall negotiate any amendments to this DPA in good faith in the event of any changes in Data Protection Laws that would necessitate such amendment with a view to agreeing and implementing those changes that are required to address the changes in Data Protection Laws as soon as is reasonably practicable.

Last Updated: July 21, 2022

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

Module 2: Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 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 select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e)

(iv) Clause 12 –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.

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 its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational

measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15

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

15.1 Notification

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

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred

pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Finland.

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 Finland.

(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

of Exhibit A

A. LIST OF PARTIES

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

1. Name: as set forth on the applicable Quote

   Address: as set forth on the applicable Quote

   Contact person's name, position and contact details: as set forth on the applicable Quote

   Activities relevant to the data transferred under these Clauses: See Agreement

   Role (controller/processor): controller

Data importer(s):

1. Name: PerkinElmer Informatics, Inc.

   Address: 940 Winter Street, Waltham, MA 02451

   Contact person's name, position and contact details: Please contact your account representative with any questions or concerns related to these Clauses, and he/she/they will direct your inquiry accordingly.

   Activities relevant to the data transferred under these Clauses: PerkinElmer is providing Customer a license to access and use the software-as-a-service offering set forth on the applicable Quote ("Service"), which will process certain personal data as described below within the application. Customer acknowledges and agrees that Customer will dictate and be responsible for the submission or input of personal data into the Service, and that, once running, the Service will operate independently and without interference or access by PerkinElmer, other than in the context of potentially providing professional services or technical support to Customer, whereby Customer will be able to determine the personal data to which PerkinElmer has access. PerkinElmer's hosting and provision of the Service, including any professional services or technical support requested by Customer, shall be deemed Customer's documented instructions for the processing of personal data. PerkinElmer will not otherwise process such personal data as uploaded into the Service without Customer's approval. Customer acknowledges that there may be certain limitations of the Service (including, for example, an inability to delete personal data in multi-tenant solutions, which instead shall be rendered inaccessible pursuant to NIST 800:88 standards) and that PerkinElmer will comply with Customer's instructions in a commercially reasonably manner and subject to Service limitations.

   Customer acknowledges and agrees that PerkinElmer will process certain personal data of users of the Service (including first/last name and email addresses and contact information, such as Customer entity and location) in the course of implementing and deploying the Service and in

such instance, PerkinElmer will be the controller of such personal data. The terms of these Clauses shall not apply to PerkinElmer in its capacity as the data controller.

Role (controller/processor): processor

PerkinElmer DPO Contact Information: DPO@perkinelmer.com

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred: The users of the Service, as designated by Customer, including employees, agents, representatives, and contractors of Customer
2. Categories of personal data transferred: Business contact information, including first/last name, email, location, job and organizational details
3. Sensitive data transferred: none
4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is uploaded by Customer during the purchased subscription term if and as dictated or performed by Customer; personal data is retained by the Service until the personal data is deleted/rendered inaccessible following the expiration or termination of the Services term in accordance with contract governing the use of the Service.
5. Nature of the processing: Personal data will be processed as necessary to provide the Service, including hosting, import, export, retrieval, access and deletion as such actions are performed by Customer users.
6. Purpose(s) of the data transfer and further processing: For performance of the Services and, if and as requested by Customer, for technical support or professional services.
7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: For the duration of the subscription term and the applicable wind-down period, as set forth in the contract governing the provision of the Service.
8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: See the list of subprocessors for the applicable Service located here: https://informatics-support.perkinelmer.com/hc/en-us/sections/4407060712212-SaaS. Personal data will be processed by such subprocessors during the term of the Agreement, and any applicable wind-down period as set forth in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Finnish Supervisory Authority

ANNEX II

of Exhibit A

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

See Global Security Addendum for Service at: https://informatics-support.perkinelmer.com/hc/en-us/sections/4407060712212-SaaS

Exhibit B

UK Addendum

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

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: PerkinElmer Informatics, Inc. Trading name (if different): N/A Main address (if a company registered address): 940 Winter St., Waltham, MA 02451 Official registration number (if any) (company number or similar identifier): 04-2897700

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Data Protection Officer Contact details including email: DPO@perkinelmer.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	X	No	General	30 days	No
3						

4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 1A of SCC to which this Addendum is attached
Annex 1B: Description of Transfer: See Annex 1B of SCC to which this Addendum is attached
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of SCC to which this Addendum is attached
Annex III: List of Sub processors (Modules 2 and 3 only): N/A, general authorisation for sub-processors

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

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

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

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

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

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

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

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

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

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

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

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

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

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

    b. its risk under the Addendum,

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

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