# Data Processing Agreement with Standard Contractual Clauses (DPA-SCC)

*Effective Date: December 5, 2024*

**Incorporated into the Agreement for the following offered Minitab Services, when applicable:**

- Minitab® Statistical Software – Web App
- Minitab Connect®
- Minitab® Real-Time SPC
- Minitab Model Ops®
- Minitab Engage®
- Minitab Education Hub™

---

**Data Processing Agreement**

This Data Processing Agreement ("**DPA**") sets forth confidentiality, security, and data privacy requirements with respect to Personal Data that is Processed by you ("**You**") and by Minitab, LLC ("**Minitab**") in connection with the provision by Minitab of the Services. This DPA constitutes a data processing agreement for the purposes of Applicable Data Protection Law. This DPA is deemed part of the Agreement. The provisions of this DPA will apply if there is any conflict between this DPA and the Agreement. Unless otherwise defined in this DPA, all capitalized terms used in this DPA have the meanings given to them in the Agreement.

**1. DEFINITIONS.**

For the purposes of this DPA unless the context requires otherwise, the following terms have these meanings:

1.1 "**DPA Effective Date**" means the date the Service is first launched or as listed in the purchase confirmation, receipt, and/or on the invoice You receive from Us for the Service.

1.2 "**Agreement**" means the Subscription Agreement between You and Minitab, LLC or its affiliate, or any other agreement, for the Service, in effect as of the DPA Effective Date between Minitab and You.

1.3 "**Applicable Data Protection Law**" means all federal, state, regional, territorial, national and local laws, regulations, and rules by any government, agency or authority that relate to the Processing or the security of Personal Data and which are applicable to Minitab or the Processing of Personal Data by You. For the avoidance of doubt this includes, where applicable, GDPR.

1.4 "**Controller**" shall have the meaning given to this term in article 4 of the GDPR, i.e., the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.5 "**Data Subject**" shall have the meaning given to this term in article 4 of the GDPR, i.e., an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.6 "**DPA Applicable Data**" shall mean any Personal Data included in Your Content and User Credentials as defined in the Agreement, or other Personal Data required for access or use of the Services.

1.7 "**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council.

1.8 "**Personal Data**" shall have the meaning given to this term in article 4 of GDPR, i.e., any information relating to an identified or identifiable natural person.

1.9 "**Personal Data Breach**" shall have the meaning given to this term in article 4 of GDPR, i.e., a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.10 "**Processing**" (and "**Process**") shall have the meaning given to this term in article 4 of the GDPR, i.e., any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Processor**" shall have the meaning given to this term in article 4 of the GDPR, i.e., a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

1.12 "**Services**" means the services subscribed to by You in accordance with the Agreement and provided by Minitab in a software as a services ("SaaS") mode.

1.13 "**Standard Contractual Clauses**" or "**SCCs**" shall mean the standard contractual clauses for the transfer of personal data from third countries pursuant to the GDPR adopted under Commission Decision 2021/914 of 4 June 2021, or the current European Commission approved version of such clauses, permitting transfers of Personal Data to Processors established outside the EU.

1.14 "**Sub-Processor**" means any party, other than an employee of Minitab, appointed by Minitab, or by any other Sub-Processor of Minitab, with whom Minitab enters into a contract, agreement or arrangement whereby it agrees to receive from Minitab, or from any other Sub-Processor of Minitab, DPA Applicable Data exclusively with the intention for Processing to be carried out on behalf of You in accordance with its instructions, the terms of the Agreement and the DPA.

1.15 "**Supervisory Authority**" shall have the meaning given to this term in article 4 of the GDPR and which has jurisdiction over Minitab's or Processor's Processing of Personal Data.

## 2. RELATIONSHIP OF THE PARTIES.

2.1 This DPA governs the manner in which DPA Applicable Data shall be Processed. Minitab is the Processor of DPA Applicable Data and You are the Controller of DPA Applicable Data under the Agreement.

2.2 The Services are provided by Minitab on a SaaS model and where You bring Your own data and largely control the upload and handle directly the use of DPA Applicable Data by the Services. In this respect, You agree and understand that Minitab will not monitor DPA Applicable Data or Your use, unless You explicitly request by writing Minitab to access a specific and well identified data or set of data in DPA Applicable Data. In any other case, only You know what data is comprised in DPA Applicable Data. It is therefore the sole liability of You to ensure that DPA Applicable Data is collected and transmitted to Minitab in compliance with Applicable Data Protection Law and, in particular, to have a legal basis for Processing and to have properly informed Data Subjects of the collection and Processing of their Personal Data.

## 3. GENERAL PERSONAL DATA OBLIGATIONS.

3.1 The Parties shall comply with the terms of this DPA, and Applicable Data Protection Law relating to the collection or Processing of Personal Data.

3.2 Minitab shall Process DPA Applicable Data solely as necessary to perform its obligations under the Agreement (or as otherwise agreed in writing by Minitab and You) on behalf of You and strictly in accordance with the documented instructions You provide and Applicable Data Protection Law (the "**Permitted Purposes**"). If Minitab is legally required to Process DPA Applicable Data otherwise than as instructed by You, it shall inform You before such Processing occurs, unless the law requiring such Processing prohibits Minitab from informing You on an important ground of public interest, in which case it shall notify You as soon as that law permits it to do so.

3.3 Additional instructions outside the scope of this DPA (if any) require prior written agreement between Minitab and You, including agreement on any additional fees payable by You to Minitab for carrying out such instructions. You shall ensure that Your instructions comply with laws, rules and regulations applicable in relation to DPA Applicable Data and that the Processing of this data in accordance with Your instructions will not cause Minitab to be in breach of Data Protection Law and, in particular, of the GDPR.

3.4 Minitab shall notify You about any instruction from You which, in its opinion, infringes Applicable Data Protection Law.

## 4. CONFIDENTIALITY OBLIGATIONS.

4.1 Minitab shall ensure that any person that it authorizes to Process Personal Data (including but not limited to Minitab's employees, contractors and other individuals engaged to provide the Services) ("**Authorized Personnel**") shall be subject to a strict duty of confidentiality, including without limitation any obligations of confidentiality that are set forth in the Agreement, and shall not permit any person who is not under such a duty of confidentiality to Process Personal Data. Minitab shall ensure that all Authorized Personnel use Personal Data solely to the extent necessary for the Permitted Purposes.

4.2 Minitab shall:

4.2.1 not publish, disclose, divulge or otherwise permit third parties to access Personal Data except in accordance with this DPA or with Your prior written consent; and

4.2.2 treat all DPA Applicable Data as confidential information.

4.3 If Minitab is required by Data Protection Law to disclose any of DPA Applicable Data to a governmental authority then it shall be entitled to do so provided that:

4.3.1 to the extent permitted by Applicable Data Protection Law, Minitab provides prior written notice of such disclosure to You without undue delay and that notice shall include a copy of the request and any related documents;

4.3.2 Minitab takes lawful actions to avoid, and minimize the extent of, that disclosure;

4.3.3 to the extent possible, Minitab receives confidentiality undertakings in a form approved by You from the entity to whom DPA Applicable Data is disclosed; and

4.3.4 before disclosing DPA Applicable Data to the governmental authority Minitab reasonably cooperates with You to resist that disclosure if You choose to do so. Where Minitab is legally prohibited from notifying You of the disclosure, Minitab shall use reasonable efforts to request the governmental authority to direct the request directly to You.

**5. COOPERATION.**

5.1 Minitab shall provide all reasonable and timely assistance to You:

5.1.1 to enable You to respond to any request from a Data Subject to exercise any of their rights under Applicable Data Protection Law (including without limitation rights of access, correction, objection, erasure and data portability, as applicable);

5.1.2 where applicable by virtue of Article 28(3) of the GDPR, to provide reasonable cooperation and assistance to You with any data protection impact assessments which are referred to in Article 35 of the GDPR or with any regulatory consultations that is legally required to make in respect of Personal Data contained within DPA Applicable Data, taking into account the nature of the Processing and the information available to Minitab.

5.1.3 upon Your request, in the event of an investigation by or request from any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation or request relates to Personal Data contained within DPA Applicable Data. Minitab will take steps reasonably requested by You to assist You in complying with any obligations in connection with such an investigation or request.

5.2 Minitab may charge You for its cooperation and assistance set forth in this DPA, which goes beyond the reasonable standards, and which will require more than reasonable efforts to comply with.

**6. DATA TRANSFERS.**

6.1 Where there are transfers of Personal Data contained within DPA Applicable Data from a Member State of the EU or from a Member State of the EEA to a third country outside the EU and outside the EEA, You and Minitab acknowledge that steps must be taken to ensure that such data transfers comply with Applicable Data Protection Law. You and Minitab acknowledge that the same or similar

obligations can apply for international transfers of Personal Data from a non-EU country and shall in good faith take the steps required where necessary under Applicable Data Protection Law.

6.2 In order to ensure that adequate safeguards are in place for Processing and transfer of Personal Data contained within DPA Applicable Data, You and Minitab hereby agree to enter into the SCCs and Minitab undertakes to enter into data processing agreements with its service providers, including Sub-Processors, that incorporate the SCCs adopted by the European Commission.

## 7. SECURITY.

7.1 Minitab will maintain and use appropriate technical and organizational measures to prevent unauthorized access to or use of the Personal Data, and to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of information or data that Minitab processes in the course of providing the Services.

7.2 Such safeguards shall include, in accordance to the article 28 (3) (c) of the GDPR, but are not limited to (a) security management policies and procedures including incident management procedures to address security events; (b) access controls, including password change controls, to ensure access to information is granted on a need to know and least privileged basis; (c) device and software management controls to guard against viruses and other malicious or unauthorized software; (d) industry standard encryption safeguards as appropriate and where required by law; (e) security awareness training to ensure employees understanding of their responsibilities in guarding against security events and unauthorized use or access to information; (f) logging procedures to proactively record user and system activity for routine review; and (g) facility access and protection controls to limit physical access to information resources and guard against environmental hazards (e.g., water or fire damage).

7.3 Minitab shall document its security measures in written form and shall make those documents available to You upon reasonable request.

## 8. PERSONAL DATA BREACH.

8.1 Minitab will notify You of a Personal Data Breach without undue delay, after it is notified, discovers, or would have discovered had it exercised reasonable diligence.

8.2 As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Minitab, Minitab will also provide You with (a) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (b) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (c) where possible, information about the types of Personal Data that were the subject of the Personal Data Breach.

8.3 You agree to coordinate with Minitab on the content of Your intended public statements or required notices for the affected individuals and/or notices to the relevant regulators regarding the Personal Data Breach.

8.4 Unless legally required by Data Protection Laws, Minitab will not disclose the Personal Data Breach to any third party without first obtaining Your prior written consent.

## 9. DELETION OR RETURN OF PERSONAL DATA.

9.1 Upon termination of the Services, and upon Your request in accordance with terms of Your Agreement, Minitab will promptly return or delete any remaining copies of Personal Data on Minitab's systems or Services environments, except as otherwise stated in the Agreement.

## 10. AUDIT.

10.1 Minitab shall permit an independent Certified Public Accountant engaged by You ("**Auditor**") to audit Minitab's compliance with this DPA, and shall make available to You and Auditor information, systems and staff necessary to conduct such audit and to demonstrate compliance with Applicable Data Protection Law. Your Auditor shall be subject to a confidentiality and non-disclosure agreement in form and substance reasonably acceptable to Minitab, and subject to Minitab's approval, which will not be unreasonably withheld. Minitab agrees that You and Auditor may enter its premises solely for the limited purpose of conducting this audit, provided that You give reasonable written prior notice, conduct the audit at a mutually agreeable time during normal business hours, and take all reasonable measures to prevent unnecessary disruption to Minitab's operations. You will not exercise this audit right more than once in any 12-month period, except (a) if and when required by a competent data protection authority or other regulator; or (b) if You believe a further audit is necessary due to a Personal Data Breach.

## 11. SUB-PROCESSORS.

11.1 Minitab may sub-contract any Processing of DPA Applicable Data performed on behalf of You under this DPA and the Agreement. You hereby grant Minitab a general authorization to engage Sub-Processors in connection with the performance of the Services by Minitab.

11.2 To the extent Minitab engages Sub-Processors to Process DPA Applicable Data, such entities shall be subject to the same level of data protection and security as Minitab under this DPA provided that each permitted subcontractor that receives DPA Applicable Data is subject to an agreement which impose privacy, confidentiality and data security obligations on the subcontractor.

## 12. SURVIVAL.

12.1 This DPA survives termination or expiration of the Agreement.

## STANDARD CONTRACTUAL CLAUSES

Controller to Processor

### SECTION I

***Clause 1***

**Purpose and scope**

1. 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 data to a third country.
2. The Parties:
    1. 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
    2. 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').
3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
4. 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**

1. 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.
2. 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**

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    2. Clause 8.1(b), 8.9(a), (c), (d) and (e);
    3. Clause 9(a), (c), (d) and (e);
    4. Clause 12(a), (d) and (f);
    5. Clause 13;

6. Clause 15.1(c), (d) and (e);
7. Clause 16(e);
8. Clause 18(a) and (b).

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

***Clause 4***
**Interpretation**

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***
**Hierarchy**
In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6***
**Description of the transfer(s)**
The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7***
[Intentionally Omitted]

**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**

1. 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.
2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

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

**8.3 Transparency**
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business

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

**8.4 Accuracy**

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

**8.5 Duration of processing and erasure or return of data**

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

**8.6 Security of processing**

1. 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.
2. 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.
3. 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.

4. 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:

1. 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;
2. 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;
3. 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
4. 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**

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
2. 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.
3. 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.
4. 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.

5. 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**

1. 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 15 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.
2. 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.
3. 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.
4. 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.
5. 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**

1. 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.
2. 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.
3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

***Clause 11***

**Redress**

1. 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.
2. 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.
3. 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:
    1. 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;
    2. refer the dispute to the competent courts within the meaning of Clause 18.
4. 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.
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. 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**

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

1. 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.
2. 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**

1. 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.
2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
    1. 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;
    2. 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;
    3. 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.
3. 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.
4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
5. 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).

6. 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**

1. 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:
    1. 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
    2. 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.
2. 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.
3. 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.).
4. 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.
5. 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**

1. 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).

2. 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.
3. 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**

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. 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).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    1. 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;
    2. the data importer is in substantial or persistent breach of these Clauses; or
    3. 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.
4. 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.
5. 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 France.

***Clause 18***

**Choice of forum and jurisdiction**

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of France.
3. 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.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):**

The individual or entity that has entered into the agreement with data importer for the provision of application(s) as described in the agreement.

Activities relevant to the data transferred under these Clauses: Uploading of data into the application(s) of processor, including user credentials to access the application(s).

Role (controller/processor): Controller

**Data importer(s):**

Name: Minitab, LLC

Address: 1829 Pine Hall Road, State College, PA 16801 USA

Contact: Data Protection Officer, DPO@minitab.com, +1 814-238-3280

Activities relevant to the data transferred under these Clauses: Processing of data uploaded into the application(s) by data exporter.

Role (controller/processor): Processor

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

- The data subjects may include the data exporters customers, employees, suppliers, end-users, and other individuals included in content uploaded to the application(s), including user credentials.

*Categories of personal data transferred*

- The data exporter determines the categories of personal data included, if any, in the content uploaded to the application(s), including user credentials.

*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.*

- Not Applicable.

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

- The data exporter determines the frequency of the transfer through their use of the application(s).

*Nature of the processing*

- The processing of personal data referred to under these Standard Contractual Clauses shall occur throughout the term of this Standard Contractual Clauses and the provision of application(s).

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

- To provide the application(s) as described in the agreement.

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

- Please see the applicable section of processors application agreement.

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

- The data exporter determines the subject matter, nature, and duration of processing of persona data transferred to sub-processor(s).

## C. COMPETENT SUPERVISORY AUTHORITY

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

- The Commission Nationale de l'Informatique et des Libertés or CNIL

  Address
  3 place de Fontenoy
  TSA 80175
  75334 Paris Cedex 07

  Telephone
  01 53 73 22 22
  01 53 73 22 00

  Website
  www.cnil.fr

## ANNEX II

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

*Effective Date: December 5, 2024*

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

*Measures of pseudonymisation and encryption of personal data*

- Pseudonymization: Pseudonymization is not applicable to data processed in the application(s).

- Encryption: For applications where data is stored, personal data in application(s) is encrypted in transit and at rest. Personal data is encrypted for transit both to and from the data exporter and for any server-to-server communication necessary for the normal functioning of the application(s). The application(s) uses only private asymmetric keys and prohibits the use of master symmetric keys. Data at rest is encrypted and protected by access controls. Only authenticated users can read, modify, or delete data as specified by the permissions associated with their account.

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

- Disaster recovery plans, including backups, are in place for all application(s). For applications where data is stored, all employees of processor, by written policy, are prohibited from accessing a
  users' account without express written permission from the user or the data exporter.

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

- Disaster recovery plans, including backups, are in place for all application(s) and are tested at least annually.

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

- During each phase of application(s) development, security measures are in place to identify and manage potential vulnerabilities throughout development and release, unless otherwise mutually agreed to by the Controller and the Processor. These include, but are not limited to:
  - OWASP Top 10 Vulnerabilities
  - Security and Privacy Risk Assessments
  - Threat Modelling
  - Static Code Analysis

- Third-Party Penetration Testing

*Measures for user identification and authorisation*

- User accounts are established in the processors license portal by data exporters' authorized representative(s). The following features exist to support the security of the accounts, unless otherwise mutually agreed upon by the Controller and the Processor:
  - Privilege Levels
  - Password Complexity
  - Automatic sign out
  - Failed Log-Ins Restrictions
  - Account De-Activation
- Once accounts are established, processor offers two methods of user authentication: 1) Password-based authentication through the processors license portal; and 2) Authentication through a third-party identity provider.
- Users application(s) permission levels are managed from within the license portal for all methods of authentication.
- Authentication within processors license portal
  - A data exporter may authenticate within the processors license portal, and users will access their applications(s) with a unique username and password set directly by the user. Strength and complexity requirements are enforced. To further secure account access, passwords are stored in an encrypted format.
- Deferred Authentication/Single Sign On (DA/SSO)
  - A data exporter may use an authentication service that provides one set of login credentials for their users to access all their applications.

*Measures for the protection of data during transmission*

- For data in transit, Minitab products use Transport Layer Security (TLS) protocol to keep data private as it moves from one location to another. This includes a Secure Sockets Layer (SSL) certificate (TLS1.2 minimum, 2048 bit key) and encryption (using RSA / AES256) for transit both to and from the customer and for any server-to-server communication necessary for the normal functioning of the application. The application uses only private asymmetric keys and prohibits the use of master symmetric keys. The following products and systems use TLS for encryption of in transit data:
  - Minitab Engage®
  - Minitab Connect®
  - Real-Time SPC
  - Minitab Model Ops®
  - Minitab® Statistical Software (Web App)

*Measures for the protection of data during storage*

- Minitab products that include storage of data on the cloud use Microsoft Azure Storage. Azure Storage uses server-side encryption (SSE) to automatically encrypt data when it is persisted to the cloud. The data is encrypted and decrypted using 256-bit AES encryption, which is FIPS 140-2 compliant. The following products and Systems use Azure Storage:
  - Minitab Engage®
  - Minitab Connect®

    - Real-Time SPC
    - Minitab Model Ops®
- For additional details on Azure Storage encryption, please see: https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption.
- For additional details on MySQL encryption, please see: https://learn.microsoft.com/en-us/azure/mysql/flexible-server/concepts-customer-managed-key

*Measures for ensuring physical security of locations at which personal data are processed*

- Minitab does not process data onsite and uses sub-processors.
- Please see Annex III.

*Measures for ensuring events logging*

- Security logs capture the following events:
    - User, system, or process identifier that triggered the event
    - Description of event
    - Date and time of event
    - Authorization information associated with the event
- Security logs, which are protected from modification and destruction, are maintained for at least 90 days.

*Measures for ensuring system configuration, including default configuration*

- Infrastructure as Code (IaC) is utilized to create, modify, and manage infrastructure in Azure, ensuring that all systems can be deployed and promoted without manual configuration. This applies the same level of rigor to infrastructure as to the codebase, including automated testing, peer review for every change, and third-party penetration testing.

*Measures for internal IT and IT security governance and management*

- The processor maintains an information security management system (ISMS), including risk management, change control, incident management, corrective measures and management oversight.

*Measures for ensuring data quality Measures for ensuring limited data retention*

- Please see the applicable section of processors application agreement.

*Measures for ensuring accountability*

- All employees of processor are trained and must acknowledge processors cybersecurity policies. Compliance with policy is monitored and retraining is provided as needed.
- All engineering staff of processor are formally trained on processors Secure Development Lifecycle. Processor performs static analysis of application code and requires manual review of source code for each application.

*Measures for allowing data portability and ensuring erasure*

- Please see the applicable section of processors application agreement.

*For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

- Processor maintains agreements with all sub-processors identified in Annex III requiring technical and organizational measures no less than those maintained by processor. Agreements contain additional terms including, but not limited to, providing assistance to the controller, processor, and data exporter as may be necessary.

## ANNEX III

## LIST OF SUB-PROCESSORS

*Effective Date: December 5, 2024*

The Controller has authorized the use of the following sub-processors:

1. **Microsoft Azure**
   Address: One Microsoft Way, Redmond, WA 98052 USA
   Contact: Chief Privacy Officer - +1 425-882-8080
   https://www.microsoft.com/en-us/concern/privacy,

   *Applications:*
   Minitab® Statistical Software – Web App
   Minitab Engage®
   Minitab Education Hub™
   Minitab Model Ops®
   Minitab Connect®
   Minitab® Real-Time SPC

   *Subject Matter*
   Your Content as defined in Annex I.
   User Credentials and other PII processed within the Service(s) provided as defined in the applicable Agreement.

   *Nature of Processing*
   Provision and performance of the Service(s) provided.

   *Location of Processing*
   USA*
   **If specifically designated in the signed Customer Agreement, Your Content may be processed in an alternate region. (Note: exceptions will occur as necessary to investigate issues of fraud and abuse). All data relating to User Credentials and other PII processed within the Service(s) is processed in the United States.*

2. **SendGrid (Twilio)**
   Address: 1801 California Street, Denver, CO 80202 USA
   Contact: Chief Privacy Officer - Twilio Privacy Team - privacy@twilio.com

   *Applications:*
   Minitab® Statistical Software – Web App
   Minitab Engage®
   Minitab Model Ops®
   Minitab Connect®
   Minitab® Real-Time SPC

   *Subject Matter*

User Credentials and other PII processed within the Service(s) provided as defined in the applicable Agreement.

*Nature of Processing*

Routing and transmission of emails.
Provision and performance of the Service(s) provided.

*Location of Processing*

USA

3. **OneTrust**

Address: 1200 Abernathy Rd NE, Atlanta, GA 30328, USA
Contact: Data Privacy Officer - DPO@onetrust.com

*Applications:*

Minitab® Statistical Software – Web App
Minitab Engage®
Minitab Model Ops®
Minitab Connect®
Minitab® Real-Time SPC

*Subject Matter*

PII processed within the Service(s) provided as defined in the applicable Agreement.

*Nature of Processing*

Provision and performance of the Service(s) provided.

*Location of Processing*

USA

4. **Docebo Inc**.

Address: 366 Adelaide Street West, Suite 701, Toronto, ON M5V 1R9, Canada
Business Number - 77293 3529
Contact: Chief Privacy Officer - privacy@docebo.com

*Applications:*

Minitab Education Hub™

*Subject Matter*

Your Content as defined in Annex I.
User Credentials and other PII processed within the Service(s) provided as defined in the applicable Agreement.

*Nature of Processing*

Routing and transmission of emails.
Provision and performance of the Service(s) provided.

*Location of Processing*

USA

**Addendum 1**

**International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

*Effective Date: December 5, 2024*

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

**Part 1: Tables**

Table 1: Parties

| **Start date** | | |
|---|---|---|
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | Full legal name:<br>Minitab, LLC<br><br>Main address:<br>1829 Pine Hall Road<br>State College, PA 16801 USA<br><br>Official registration number:<br>Z6501566 | The individual or entity that has entered into the agreement with data importer for the provision of application(s) as described in the agreement. |
| **Key Contact** | Full Name (optional):<br>Dan Michaeli<br><br>Job Title:<br>Vice President of Data Protection & Intellectual Property<br><br>Contact details including email:<br>DPO@minitab.com<br>814-238-3280 | The individual or entity that has entered into the agreement with data importer for the provision of application(s) as described in the agreement. |

Table 2: Selected SCCs, Modules and Selected Clauses

| **Addendum EU SCCs** | ☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: December 1, 2022 |
|---|---|

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 Page 21 of the Data Processing Agreement with Standard Contractual Clauses. |
| Annex 1B: Description of Transfer: See Page 21 of the Data Processing Agreement with Standard Contractual Clauses. |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Page 23 of the Data Processing Agreement with Standard Contractual Clauses. |
| Annex III: List of Sub processors (Modules 2 and 3 only): See Page 27 of the Data Processing Agreement with Standard Contractual Clauses. |

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:<br>☒ Importer<br>☒ Exporter<br>☐ 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.