Quantum

Data Processing Addendum

This Data Processing Addendum (*"**Addendum**"*) supplements the Quantum Sales and Support Terms and Conditions available at *www.Quantum.com*, or other agreement between Customer and Quantum governing Customer's use of the Quantum Products or Services (the *"**Agreement**"*) and reflects the Party's agreement with regard to the processing of Personal Information in accordance with the requirements of the applicable Data Privacy and Security Laws. The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. This Addendum forms part of the Agreement and will have the same force and effect as if set out in the body of the Agreement.

1. DEFINITIONS AND INTERPRETATIONS

The following terms shall have the following meanings:

(a) *"**Affiliate**"* means, in relation to either Customer or Quantum, an entity that owns or controls, is owned or controlled by or is under common control or ownership with Customer or Quantum (as applicable), 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;

(b) *"**Applicable Law**"* means all applicable laws, statutes, codes, ordinances, decrees, rules, regulations, municipal by-laws, judgments, orders, decisions, rulings or awards of any government, quasi-government, statutory or regulatory body, ministry, government agency or department, court, agency or association of competent jurisdiction;

(c) *"**Controller**"* means an entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Information, and shall also mean a *"**Business**"*, where applicable, as defined by the CCPA;

(d) *"**Customer Personal Information**"* shall have the meaning given to it in Section 0;

(e) *"**Data Privacy and Security Laws**"* means all laws and regulations applicable to the processing of Personal Information under the Agreement, including, as applicable, laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States, governing the privacy, data protection and security of Personal Information and security breach notification. Data Privacy and Security Laws shall include the GDPR and the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 –1798.199, and its implementing regulations (the "***CCPA***"), each as amended, repealed or replaced from time to time;

(f) *"**GDPR**"* means Regulation (EU) 2016/679 and also refers to the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (*"**UK GDPR**"*) (in this Addendum, any references to specific articles of the GDPR shall be construed as also referring to the equivalent sections of the UK GDPR, where applicable);

(g) *"**Personal Information**"* means any information relating to an identified or identifiable natural person (a "***Data Subject***") and/or any such information as may be defined as constituting Personal Information,

personally identifiable information or any equivalent thereof, in any applicable Data Privacy and Security Laws;

(h) *"**Process**"* and variants of it, such as "***processing***" and "***processed***" (whether capitalized or not) means any operation or set of operations performed upon Personal Information or sets of Personal Information, 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;

(i) *"**Processor**"* means an entity which processes Personal Information on behalf of the Controller and shall also mean a "***Service Provider***", where applicable, as defined by the CCPA;

(j) *"**Standard Contractual Clauses**"* means the standard contractual clauses for the transfer of Personal Information to processors established in third countries, as approved by the European Commission in Decision (EU) 2021/914 as set out in Schedule A;

(k) *"**Subprocessor**"* means any person or entity appointed by or on behalf of Quantum (or the relevant intermediate Subprocessor) to process Personal Information as described in Section 6; and

(l) *"**Supervisory Authority**"* means a supervisory authority established by an EEA Member State or the United Kingdom, pursuant to Article 51 of the GDPR, or any other competent government authority with jurisdiction over the processing of Personal Information under the Agreement.

In this Addendum (except where the context otherwise requires any phrase introduced by the terms "**including**", "**include**", "**in particular**" or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

2. ROLES OF THE PARTIES

Both parties will comply with all applicable requirements of the Data Privacy and Security Laws. This Section 0 is in addition to, and does not relieve, remove or replace, either party's obligations under the Data Privacy and Security Laws.

The parties acknowledge and agree that for the purposes of the Data Privacy and Security Laws, Customer is the Controller and Quantum is the Processor.

Customer shall ensure that it has and will continue to have, the right to transfer, or provide access to, Customer Personal Information to Quantum for processing in accordance with the Agreement. For the avoidance of doubt, Customer's instructions for the processing of Customer Personal Information shall comply with applicable Data Privacy and Security Laws. Quantum will inform Customer if it considers, in its opinion, that any of Customer's instructions infringe applicable Data Privacy and Security Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Information and the means by which Customer acquires Customer Personal Information and shall be responsible for ensuring that the processing of Personal Information, which Quantum is instructed to perform, has a valid legal basis.

3. SCOPE OF PROCESSING

Customer agrees that Quantum may process Personal Information on behalf of Customer to perform its obligations under the Agreement for the term of the Agreement ("**Customer Personal Information**") in accordance with this Addendum. A list of the categories of data subjects, types of Customer Personal Information and the processing activities are set out in Appendix I to the Standard Contractual Clauses. The duration of the processing corresponds to the term of the Agreement, unless otherwise stated in the Agreement or this Addendum.

Quantum shall process Customer Personal Information only on the written instructions of Customer unless Quantum is required by Applicable Law to process such data. Where Quantum is relying on Applicable Law as the basis for processing Customer Personal Information, Quantum shall notify Customer of this before performing the processing required by Applicable Law unless Applicable Law prohibits Quantum from so notifying Customer.

The following is deemed an instruction by Customer to process Customer Personal Information, subject to Quantum's compliance with this Addendum and the Data Privacy and Security Laws: (i) processing necessary for Quantum's performance of its obligations under the Agreement; (ii) processing initiated by Customer, an Authorized Customer Entity or an Authorized User in their use of the Products or Services; and (iii) processing necessary to comply with other reasonable instructions provided by Customer where such instructions are consistent with the Agreement and this Addendum.

4. DATA PROCESSING OBLIGATIONS

Without prejudice to the generality of Section 0, Quantum shall, in relation to any Customer Personal Information processed in connection with the performance by Quantum of its obligations under the Agreement:

(a) maintain technical and organizational measures designed to protect against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Information in its possession or control (a "**Personal Information Breach**");

(b) ensure that all personnel who have access to and/or process Customer Personal Information are obliged to keep Customer Personal Information confidential;

(c) taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, in responding to a request from a Data Subject and in ensuring compliance with its obligations under the Data Privacy and Security Laws with respect to records of processing, security, breach notifications, impact assessments and consultations with Supervisory Authorities. To the extent legally permitted, Customer shall be responsible for any costs arising from Quantum's provision of such assistance;

(d) notify Customer without undue delay on becoming aware of a Personal Information Breach and shall provide Customer with further information about the Personal Information Breach in phases as such information becomes available to Quantum; and

(e) at the written direction of Customer, delete or return Customer Personal Information and copies thereof in its possession or control to Customer on termination of the Agreement unless required by Applicable Law to store Customer Personal Information.

Quantum shall maintain records and information to demonstrate its compliance with this Addendum. Customer shall, with reasonable notice to Quantum, have the annual right (unless required more frequently by an order of a Supervisory Authority or court, or in the event of a Personal Information Breach) to review such records at Quantum's offices during regular business hours.

Upon Customer's request, Quantum shall, no more than once per calendar year (unless required more frequently by an order of a Supervisory Authority or court, or in the event of a Personal Information Breach) make available for Customer's review copies of certifications or reports demonstrating Quantum's compliance with this Addendum and the prevailing data security standards applicable to the processing of Customer Personal Information.

Where Customer reasonably believes the information provided under Section 0 and 0 above is not sufficient to demonstrate Quantum's compliance with this Addendum, at Customer's expense and subject to Section 5, Quantum shall permit Customer, or its appointed third-party auditors (collectively, "**Auditor**"), to audit the architecture, systems and procedures

relevant to Quantum's compliance with this Addendum and shall make available to the Auditor all information, systems and staff necessary for the Auditor to conduct such audit. To the extent any such audit incurs in excess of 10 hours of Quantum personnel time, Quantum may charge Customer on a time and materials basis for any such excess hours.

5. AUDITS

Before the commencement of an audit described in Section 4, Quantum and Customer will mutually agree upon the reasonable scope, start date, duration of and security and confidentiality controls applicable to the audit. Customer agrees that:

(a) audits will be conducted during Quantum's normal business hours;

(b) it will not exercise its on-site audit rights more than once per calendar year, (unless required more frequently by an order of a Supervisory Authority or court, or in the event of a Personal Information Breach);

(c) it will be responsible for any fees charged by any third party auditor appointed by Customer to execute any such audit;

(d) Quantum may object to any third-party auditor appointed by Customer to conduct an audit if the auditor is, in Quantum's opinion, not suitably qualified or independent, a competitor of Quantum or otherwise manifestly unsuitable. Any such objection by Quantum will require Customer to appoint another auditor or conduct the audit itself;

(e) nothing in this Section 5 will require Quantum either to disclose to the Auditor, or to allow the Auditor access to (a) any data processed by the Quantum on behalf of any other organisation, (b) any Quantum internal accounting or financial information, (c) any trade secret of Quantum, (d) any information that, in Quantum's opinion, could (i) compromise the security of any Quantum systems or premises, or (ii) cause Quantum to breach its obligations to Customer or any third party, or (e) any information that Customer seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Applicable Data Protection Law; and

(f) shall provide Quantum with copies of any audit reports completed by the Auditors, which reports shall be subject to the confidentiality provisions of the Agreement.

6. APPOINTMENT OF SUBPROCESSORS

Customer authorizes Quantum to appoint (and permit each Subprocessor appointed in accordance with this Section 6 to appoint) Subprocessors in accordance with this Section 6 and any restrictions in the Agreement.

Quantum may continue to use those Subprocessors already engaged by Quantum, subject to Quantum in each case as soon as practicable meeting the obligations set out in Section 6.4.

Quantum shall give Customer prior notice of any intended changes concerning the appointment or replacement of Subprocessors. If, within fourteen (14) days of receipt of that notice, Customer notifies Quantum in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Quantum shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Products and Services which avoids the use of that proposed Subprocessor; and

(b) where such a change cannot be made within thirty (30) days from receipt by Quantum of Customer's notice, notwithstanding anything in the Agreement, Customer may by written notice to Quantum terminate those Products and Services which cannot be provided by Quantum without the use of the objected-to Subprocessor. This termination right is Customer's sole and exclusive remedy if Customer objects to any proposed Subprocessor.

With respect to each Subprocessor, Quantum shall:

(c) ensure that the arrangement between on the one hand (a) Quantum, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Information as those set out in this Addendum and meet the requirements of Article 28(3) of the GDPR;

(d) to the extent that Subprocessor processes Customer Personal Information outside of the European Union, European Economic Area and/or the United Kingdom, Quantum will ensure that appropriate safeguards are at all relevant times incorporated into the agreement between on the one hand (a) Quantum, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first processes Customer Personal Information procure that it enters into an agreement incorporating appropriate safeguards; and

(e) provide to Customer for review such copies of the agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

Quantum may replace a Subprocessor if the need for the change is urgent and necessary to provide the Products and Services and the reason for the change is beyond Quantum's reasonable control. In such instance, Quantum shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Subprocessor pursuant to Section 0 above.

Where the Subprocessor fails to fulfil its data protection obligations and Quantum is the initial Processor, Quantum shall remain fully liable to Customer for the performance of that Subprocessor's obligations.

7. INTERNATIONAL TRANSFERS

The Parties hereby enter into the Standard Contractual Clauses with respect to any transfer of Customer Personal Information to which the GDPR and/or UK GDPR applies from Branded (as "data exporter") to Quantum (as "data importer") where such transfer would otherwise be prohibited by Data Protection Legislation. The Standard Contractual Clauses shall come into effect on the commencement of a relevant transfer as described in this Section 7.

In case of any transfers of Customer Personal Information subject to the UK GDPR, (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Privacy and Security Laws of the UK including the UK GDPR ("***UK Data Protection Laws***"), as applicable; (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws, as applicable, (iii) Clause 13(a) and Part C of Annex I are not used; (iv) the "competent supervisory authority" is the UK Information Commissioner's Office; and (v) Clause 17 is replaced to state "*These Clauses are governed by the laws of England and Wales*" and Clause 18 is replaced to state: "*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*."

In case of any transfers of Customer Personal Information subject to the Data Privacy and Security Laws or Switzerland ("***Swiss Data Protection Laws***"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws, as applicable; (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under Swiss Data Protection Laws, as applicable, (iii) Clause 13(a) and Part C of Annex I are not used; (iv) the "competent supervisory authority" is the Swiss Federal Data Protection and Information Commissioner; and (v) Clause 17 is replaced to state "*These Clauses are governed by the laws of Switzerland*".

Additional terms for Standard Contractual Clauses:

(a) For the purposes of Clause 8.1(a) of the Standard Contractual Clauses, the processing described in Section 3 of this Addendum is deemed an instruction by Customer to process Customer Personal Information, subject to Quantum's compliance with applicable Data Privacy and Security Laws.

(b) Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer agrees that Quantum may continue to use those Subprocessors already engaged by Quantum as at the date of this Addendum, subject to Quantum in each case as soon as practicable meeting the obligations set out in Section 6.4.

(c) Pursuant to Clause 9(a) of the Standard Contractual Clauses, Customer agrees that Quantum may engage new Subprocessors as detailed in Section 6 of this Addendum.

(d) Customer agrees that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Sections 4 and 5 of this Addendum.

(e) In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. The parties' signature to the Agreement shall be considered as signature to the Standard Contractual Clauses.

Quantum may propose variations to this Addendum and the Standard Contractual Clauses which Quantum reasonably considers to be necessary to address the requirements of any Data Privacy and Security Laws, and the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Quantum's notice as soon as is reasonably practicable.

8. GENERAL TERMS

Termination and Survival. The parties agree that this Addendum shall terminate automatically upon termination of the Agreement. Notwithstanding the foregoing, any obligation imposed on Quantum under this Addendum in relation to the processing of Customer Personal Information shall survive any termination or expiration of this Addendum.

Governing Law. This Addendum shall be governed by the governing law of the Agreement.

Jurisdiction. The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum.

Order of precedence. Nothing in this Addendum reduces Quantum's obligations under the Agreement in relation to the protection of Customer Personal Information or permits Quantum to process (or permit the processing of) Customer Personal Information in a manner which is prohibited by the Agreement. In the event of any inconsistency between this

Addendum and any other agreements between the parties, including but not limited to the Agreement, the Addendum shall prevail.

Severance. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

SCHEDULE A: STANDARD CONTRACTUAL CLAUSES

Schedule A is part of the DPA and must be included as part of and signed with the DPA to be valid and legally binding.

Standard contractual clauses for the transfer of personal data to third countries which do not ensure an adequate level of data protection (controller to processor transfers).

Name of the data exporting organisation: _____ (the "**Data Exporter**")

Address: _____

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation: _____

AND

Name of the data importing organisation: Quantum Corporation (the "**Data Importer**")

Address: 224 Airport Parkway, Suite 550, San Jose, California 95110, United States

Tel.: 408 944 4000; e-mail: legal@quantum.com

each a "**Party**"; together "**the Parties**",

HAVE AGREED on the following Contractual Clauses ("**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the Personal Data specified in Appendix I.

SECTION I

Clause 1

1. Purpose and Scope

1.1. 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 personal data to a third country.

1.2. The Parties:

(a) 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 *Appendix I (A)* (hereinafter each "data exporter"), and

(b) 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 *Appendix I (A)* (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

1.3. These Clauses apply with respect to the transfer of personal data as specified in *Appendix I (B)*.

1.4. The Appendix to these Clauses referred to therein forms an integral part of these Clauses.

Clause 2

2. Effect and invariability of the Clauses

2.1. 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.

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

Clause 3

3. Third-party beneficiaries

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

(a) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(b) Clause 8.1.2, 8.9.1, 8.9.3, 8.9.4 and 8.9.5;
(c) Clause 9.1, 9.3, 9.4 and 9.5;
(d) Clause 12.1, 12.4 and 12.6;
(e) Clause 13;
(f) Clause 15.1.3, 15.1.4 and 15.1.5;
(g) Clause 16.5;
(h) Clause 18.1 and 18.2.

3.2. Paragraph 3.1 is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

4. Interpretation

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

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

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

Clause 5

5. Hierarchy

5.1. 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

6. Description of the transfer(s)

6.1. 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 *Appendix I (B)*.

Clause 7

7. Docking clause

7.1. 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 *Appendix I (A)*.

7.2. Once it has completed the Appendix and signed *Appendix 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 *Appendix I (A)*.

7.3. 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

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

8.1.1. 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.

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

8.2. Purpose limitation

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

8.3. Transparency

8.3.1. 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 *Appendix 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

8.4.1. 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

8.5.1. Processing by the data importer shall only take place for the duration specified in *Appendix 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 14.5 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 14.1.

8.6. Security of processing

8.6.1. 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 *Appendix II*. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2. 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.

8.6.3. 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.

8.6.4. 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

8.7.1. 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 *Appendix I (B)*.

8.8. Onward transfers

8.8.1. 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:

(a) 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;

(b) 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;

(c) 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

(d) 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

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

8.9.2. 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.

8.9.3. 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 noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

8.9.4. 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.

8.9.5. The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.

Clause 9

9. Use of sub-processors

9.1. 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 fifteen (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.

9.2. 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.

9.3. 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.

9.4. 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.

9.5. 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

10. Date subject rights

10.1. 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.

10.2. 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 *Appendix 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.

10.3. In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the data exporter.

Clause 11

11. Redress

11.1. 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.

11.2. 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.

11.3. 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:

(a) 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;

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

11.4. 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.

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

11.6. 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

12. Liability

12.1. 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.

12.2. 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.

12.3. Notwithstanding paragraph 12.2, 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.

12.4. The Parties agree that if the data exporter is held liable under paragraph 12.3 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.

12.5. 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.

12.6. The Parties agree that if one Party is held liable under paragraph 12.5, 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.

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

Clause 13

13. Supervision

13.1. The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in *Appendix I (C)*, shall act as competent supervisory authority.

13.2. 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

14. Local laws and practices affecting compliance with the Clauses

14.1. 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.

14.2. The Parties declare that in providing the warranty in paragraph 14.1, they have taken due account in particular of the following elements:

(a) 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;

(b) 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;

(c) 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.

14.3. The data importer warrants that, in carrying out the assessment under paragraph 14.2, 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.

14.4. The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.

14.5. 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 14.1, 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 14.1.

14.6. Following a notification pursuant to paragraph 14.5, 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 16.4 and 16.5 shall apply.

Clause 15

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

15.1. Notification

15.1.1. 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:

(a) 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

(b) 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.

15.1.2. 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.

15.1.3. 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.).

15.1.4. The data importer agrees to preserve the information pursuant to paragraphs 15.1.1 to 15.1.3 for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5. Paragraphs 15.1.1 to 15.1.3 are without prejudice to the obligation of the data importer pursuant to Clause 14.5 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

15.2.1. 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 14.5.

15.2.2. 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.

15.2.3. 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

16. **Non-compliance with the Clauses and termination**

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

16.2. 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 14.6.

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

(a) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph 16.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

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

(c) 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.

16.4. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph 16.3 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.

16.5. 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

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 Belgium.

Clause 18

18. Choice of forum and jurisdiction

18.1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

18.2. The Parties agree that those shall be the courts of Belgium.

18.3. 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.

18.4. The Parties agree to submit themselves to the jurisdiction of such courts.

On behalf of the Data Exporter:	**On behalf of the Data Importer:**
[NAME]	**Quantum Corporation**
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

.

APPENDIX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

This Appendix forms part of the Clauses and must be completed and signed by the Parties.

Data exporter(s)

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

Name: ……

Address: ……

Contact person's name and position:

……

Tel.: ……; e-mail: ……

Activities relevant to the data transferred under these Clauses:

……

Role: Controller

AND

Data importer(s)

[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: Quantum Corporation

Address: 224 Airport Parkway, Suite 550, San Jose, California 95110, United States

Contact person's name and position:

……

Tel.: 408 944 4000; e-mail: legal@quantum.com

Activities relevant to the data transferred under these Clauses:

……

Role: Processor

B. DESCRIPTION OF TRANSFER

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):

- ☐ Employees
- ☐ Customers (contact persons)
- ☐ Prospects / Leads (contact persons)
- ☐ Contractors (contact persons)
- ☐ Insureds
- ☐ Patients
- ☐ None of the above
- ☐ Other: ……

Categories of Data

The Personal Data transferred concern the following categories of data (please specify):

- ☐ Social Security Numbers
- ☐ Email addresses
- ☐ Phone numbers
- ☐ Addresses
- ☐ Credit Card information
- ☐ Bank account information
- ☐ IP Addresses
- ☐ Employment data
- ☐ Job title
- ☐ Answers to surveys
- ☐ None of the above
- ☐ Other: ……

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following Special Categories of data (please specify):

- ☐ Data revealing racial origin
- ☐ Data revealing ethnic origin
- ☐ Data revealing political opinions
- ☐ Data revealing religious beliefs

- ☐ Data revealing philosophical beliefs
- ☐ Data revealing trade-union membership
- ☐ Data concerning health life
- ☐ Data concerning sex life
- ☐ None of the above
- ☐ Other: ……

Frequency of the transfer

The Personal Data will be transferred on the following basis (please specify):

- ☐ One-off
- ☐ Continuous

Processing Operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify nature of the processing, purpose(s) of the data transfer and further processing):

……
……
……

Retention

The Personal Data transferred will be retained for the following timeframe (please specify):

- ☐ …… years …… months
- ☐ The length of the data processing agreement
- ☐ The length of the data processing agreement plus …… years …… months

Transfers to sub-processors

The Personal Data transferred to sub-processors will be subject to the following Processing activities (please specify subject matter, nature and duration of the processing):

……
……
……

C. COMPETENT SUPERVISORY AUTHORITY

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

……

Data Exporter:	**Data Importer:**
[NAME]	**Quantum Corporation**
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

APPENDIX II TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the Parties.

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

The present document supplements the Art 28 GDPR (EU General Data Protection Regulation).

The technical and organizational measures are implemented by Quantum in accordance with regulatory requirements. Measures are periodically improved by Quantum according to feasibility and mitigation impact.

1. Confidentiality

1.1. Physical Access Control

Measures for preventing unauthorized persons from gaining access to Quantum data processing systems with which personal or customer data are processed or used.

Technical Measures

- Alarm system
- Automatic access control system
- Biometric access barriers
- Smartcards
- Manual locking system
- Doors with knob outside
- Video surveillance of entrances
- Card access control datacenter

1.2. Logical Access Control

Organizational Measures

- Key regulation/List
- Reception/Receptionist
- Visitors' book/Visitors' protocol
- Employee/visitor badges
- Visitors accompanied by employees
- Care in selection of cleaning services
- Instructions for operational safety
- Work instruction for access control
- Information Security Policy

Measures for preventing Quantum data processing systems from being used by unauthorized persons.

Technical Measures

- Login with username and strong password
- Anti-Virus Software on Servers
- Anti-Virus Software on Clients
- Firewall
- Intrusion Detection Systems
- Use of VPN for remote access
- Encryption of data in transit and data at rest
- Automatic desktop lock
- Encryption of laptops/iPads
- Multi-factor authentication in datacenter operation and for critical systems

Organizational Measures

- User provisioning/deprovisioning/permission management
- Creating user profiles (RBAC and ABAC)
- Central password management
- Access control
- Information Security Policy

1.3. Authorization Control

Measures to ensure that those authorized to use a Quantum data processing system can only access the data appropriate to their access authorization and that Restricted data cannot be read, copied, modified, or removed without authorization during processing, use and after storage.

Technical Measures

- Hard Drive wipe/file shredder
- External destruction of disposal media
- Physical deletion of data carriers
- Logging of access to applications, specifically when entering, changing, and deleting data
- SSH encrypted access
- Certified SSL encryption

1.4. Separation Control

Organizational Measures

- Data Classification
- Minimum number of administrators
- Management of user rights by administrators
- Data Handling guidelines
- Information Security Policy

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical Measures

- Separation of production and test environment
- Physical separation (systems / databases / data carriers)
- Multi-tenancy of relevant applications
- VLAN segmentation
- Staging of development, test, and production environment

1.5. Pseudonymization

Organizational Measures

- Control via authorization policy
- Determination of database rights
- Work instruction operational security
- Information Security Policy

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures

- Log files are pseudonymized at the request of the customer

Organizational Measures

- Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
- Specific internal controls on cryptography
- Information Security Policy

2. Integrity

2.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures

- VPN
- Logging of access and retrievals
- Provision via encrypted connections such as TLS, SFTP, HTTPS and secure cloud stores

2.2. Input Control

Organizational Measures

- VPN
- Monitor regular retrieval and transmission processes
- Transmission in anonymized or pseudonymized (encrypted) form
- Careful selection of transport personnel and vehicles
- Personal handover with protocol
- Information Security Policy

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered, modified, or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures

- Technical logging of the entry, modification, and deletion of data
- Manual or automated control of the logs (according to strict internal specifications)
- SIEM

Organizational Measures

- Survey of which programs can be used to enter, change, or delete which data
- Traceability of data entry, modification, and deletion through individual usernames (not user groups)
- Assignment of rights to enter, change and delete data based on an authorization policy
- Retention of forms from which data has been transferred to automated processes
- Clear responsibilities for deletions
- Work instruction IT admin compliance
- Information Security Policy

3. Availability and Resilience

3.1. Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

Technical Measures

- Fire and smoke detection systems
- Fire extinguisher server room
- Server room monitoring temperature and humidity
- Server room air-conditioning
- UPS system and emergency diesel generators
- Protective socket strips server room
- RAID system / hard disk mirroring
- Video surveillance server room
- Alarm message in case of unauthorized access to server room

3.2. Resiliency

Organizational Measures

- Backup
- Existence of an emergency plan
- Storage of backup media in a secure location outside the server room
- Separate partitions for operating systems and data where necessary
- Information Security Policy

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures

- Backups
- Restoration from backup automation tools
- Backup policy according to criticality

Organizational Measures

- Business Continuity and Recovery policy
- Data Backup process
- Regular testing of data recovery and logging of results
- Storage of backup media in a safe place outside the server room
- Existence of an emergency plan
- Information Security Policy

4. Procedures for Periodic Review, Assessment and Evaluation

4.1. Data Protection Management

Technical Measures

- Review of TOMs is performed annually, and TOMs are updated as technologies measures change
- Data protection checkpoints consistently implemented in tool-supported risk assessment

Organizational Measures

- Regular security awareness trainings at least annually
- Security official appointed: Director, Information Security
- Data Protection impact is carried out as part of corporate risk management
- Formalized process for requests for information from data subjects is in place
- Data protection aspects established as part of corporate risk management

4.2. Incident Response Management

Support for security breach response and data breach process.

Technical Measures

- Use of firewall and regular updating
- Use of spam filter and regular updating
- Use of virus scanner and regular updating
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

Organizational Measures

- Documented process for detecting and reporting security incidents / data breaches
- Formalized procedure for handling security incidents
- Involvement of ISO in security incidents and data breaches
- Documentation of security incidents and data breaches
- A formal process for following upon security incidents and data breaches
- Information Security Policy

4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures Organizational Measures

- No more personal data is collected than is necessary for the respective purpose
- Use of data protection-friendly default settings in standard and individual software
- Data Protection Policy (includes principles "privacy by design / by default")
- Perimeter analysis for web applications

4.4. Order Control (outsourcing, subcontractors, and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures

- Monitoring of remote access by external parties, e.g., in the context of remote support
- Monitoring of subcontractors according to the principles and with the technologies

Organizational Measures

- Work instruction supplier management and supplier evaluation
- Prior review of the security measures taken by the contractor and their documentation
- Selection of the contractor under due diligence aspects (especially regarding data protection and data security)
- Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
- Framework agreement on contractual data processing within the group of companies
- Written instructions to the contractor
- Obligation of the contractor's employees to maintain data secrecy
- Agreement on effective control rights over the contractor
- Regulation on the use of further subcontractors
- Ensuring the destruction of data after termination of the contract
  In the case of longer collaboration: ongoing review of the contractor and its level of protection

5. Organization and Data Protection at Quantum

This guideline provides the framework for transparent, sustainable, process-based, and risk-oriented management of Quantum data.

Quantum has established a distinctive cross-sectional security organization to ensure comprehensive protection of its own corporate information and data as well as protection of the data it receives from third parties. The functions of the CIO, Information Security, and Legal and Compliance Office with group-wide responsibility and direct authority in these areas of activity have been established.

Employees are trained in ethics, compliance, information security, and data protection. In addition, Quantum employees sign confidentiality agreements upon hiring. External parties who may encounter personal data in the course of their work for Quantum are obligated to maintain confidentiality requirements as well as to comply with applicable data protection regulations. All these organizational measures are augmented by Quantum's current security standards, which are periodically reviewed and confirmed for adequacy and effectiveness in the course of ongoing internal audits.

Data Exporter:	**Data Importer:**
[NAME]	**Quantum Corporation**
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

APPENDIX III TO THE STANDARD CONTRACTUAL CLAUSES

LIST OF PROCESSORS AND SUB-PROCESSORS

The controller has authorised the use of the following processors and sub-processors. This list is not exhaustive and is subject to change from time to time.

Company name	Location	Services provided
1099 Pro, Inc.	United States	Tax e-filing and corporate suite software
i-4business EMEA Limited	United Kingdom	B2B database provider
1Path	United States	Managed IT services provider
American Express	United States	Credit card provider
Bugzilla	United States	Bug tracking system
CR Worldwide	United Kingdom	Recognition and rewards platform provider
Deloitte	South Korea	Payment services
DirectPay	United States	Payment service provider
DocuSign, Inc.	United States	Electronic signature platform
E*Trade	United States	Electronic trading platform
Fidelity Investments Inc.,	United States	Financial services
FoundationIP LLC	United States	IP management software
HireRight	United States	Background screening
Impartner, Inc.	United States	Channel management platform
Joyo	China	Recognition and rewards platform provider
Lessonly, Inc.	United States	Learning management system
Marketo	United States	Marketing automation software
Microsoft Corporation	United States	File storage and cloud-based email services
N-Able Technologies International Inc	United States	IT asset management software
Oracle Corporation	United States	Enterprise resource planning software
Salesforce	United States	Customer relationship management platform
Schedule IT	United Kingdom	Scheduling software
Shinmaxx	South Korea	Recognition and rewards platform provider
Staples Inc.	United States	Office supplies provider
TimeTool	United Kingdom	Time recording and absence management software
TMF Group	Australia, Belgium, France, Germany, Italy, Japan, Korea, Spain, Malaysia, Netherlands, Singapore, Spain, Switzerland, United Kingdom	Accounting, corporate secretarial, tax and payroll services
Track-It!	United States	IT help desk software
Trade Automation	United States	Due diligence checks for export / import compliance
Tricor Global	Malaysia, Singapore	Payment services
Ultimate Kronos (UKG Group)	United States	HR and payroll software

Vartopia	United States	Partner relationship management software
WorkStride	United States	Recognition and rewards platform provider
ZoomInfo Technologies Inc.	United States	B2B database provider

The following Quantum controlled subsidiaries support, operate, deliver, and maintain Quantum services and in the course of doing so, may process, store, or otherwise access team member and customer data.

Company name	**Location**
A.C.N. 120 786 012 Pty Ltd	Australia
Quantum Engineering Australia Pty Ltd	Australia
Quantum Storage Australia Pty Ltd	Australia
Quantum Storage Belgium BV	Belgium
Quantum SARL	France
Quantum Beteiligungs GmbH	Germany
Quantum Bohmenkirch GmbH & Co. KG	Germany
Quantum Storage Italy, S.R.L.	Italy
Quantum Storage Japan Corporation	Japan
Quantum Korea Company Co. Ltd.	South Korea
Quantum International Inc – Malaysia Branch	Malaysia
Quantum Storage Malaysia Sdn. Bhd.	Malaysia
Quantum Storage Singapore Pte. Ltd.	Singapore
Quantum Storage Spain, S.L.	Spain
Quantum Peripherals Europe SARL	Switzerland
Quantum Storage GmbH	Switzerland
Quantum Storage UK, Ltd.	United Kingdom
Square Box Systems Limited	United Kingdom
Advanced Digital Information Corporation	United States
Certance Holdings Corporation	United States
Certance (US) Holdings Inc.	United States
Certance LLC	United States
Quantum Government Inc.	United States
Quantum International, Inc.	United States
Quantum LTO Holdings, LLC	United States