Data Processing Addendum

Last Updated: November 2024

This Data Processing Addendum and its Appendices (the "**DPA**") is an agreement between SpotQA Limited trading as 'Virtuoso QA' ("**SpotQA**") and the Customer ("**Customer**"), collectively referred to as the "**Parties**" and individually as a "**Party**". This DPA supplements and is incorporated into the underlying agreement between the Parties (the "**Customer Agreement**") and reflects the Parties' agreement with respect to the Processing of Customer Personal Data by SpotQA as a Processor on Customer's behalf in connection with the Services.

In case of any conflict or inconsistency with the terms of the Customer Agreement, this DPA will take precedence over other terms in the Customer Agreement to the extent of such conflict or inconsistency.

Terms not otherwise defined in this DPA will have the meaning as set forth in the Customer Agreement.

1. Definitions

1.1. In this DPA, the following terms have the following meanings:

"**Affiliate**" means, in relation to either Party, any entity: (a) which is owned more than 50% by that Party; or (b) over which that Party exercises management control; or (c) which is under common control with that Party; or (d) which owns more than 50% of that Party's voting securities. .

"**Applicable Data Protection Law**" means all applicable data protection legislation, including without limitation: (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (iv) Swiss Federal Act on Data Protection and its Ordinance ("**FADP**"); (iv) the California Consumer Privacy Act Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018, including as modified by the California Privacy Rights Act ("**CCPA**") and (v) any other applicable law or regulation which governs the Processing of Personal Data and the free movement of such data, and in each case, as may be amended, superseded, or replaced.

"**Authorised User**" means an individual who is authorised to use the Services (for instance individuals who have been supplied with a user identification and password by the Customer). Authorised Users may include Customer's or a Customer Affiliate's employees, consultants, contractors, agents or other third parties.

"**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**" "**Processing**" and "**Process**" shall have the meanings given in Applicable Data Protection Law.

“**Customer Data**” means data Customer submits to SpotQA in connection with the use of the Services.

“**Customer Personal Data**” means any Personal Data contained within Customer Data that SpotQA Processes as a Processor on behalf of the Customer.

"**EEA**" means the European Economic Area.

“**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise Processed by SpotQA and/or itsSub-processors in connection with the provision of the Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“**Privacy Policy**” means the Privacy Policy located at https://www.SpotQAqa.com/privacy-policy, as it may be updated by SpotQA from time to time.

“**Restricted Transfer**” means the disclosure, grant of access, or other transfer of Customer Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an “**EEA Restricted Transfer**”); (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a “**UK Restricted Transfer**”); and (iii) in the context of Switzerland, a country or territory outside of Switzerland which does not benefit from an adequacy decision from the Swiss Government (a “**Swiss Restricted Transfer**”), which would be prohibited without a legal basis under Chapter V of the GDPR and/or the FADP (as applicable to the Processing concerned).

"SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data in countries not otherwise recognised as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

“**Services**” means the services provided by SpotQA to Customer as described in the Customer Agreement.

“**UK Addendum**” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as may be amended, superseded, or replaced.

2. General

2.1. In performing the obligations under the Customer Agreement and this DPA, SpotQA will Process the Customer Personal Data on behalf of the Customer in accordance with Applicable Data Protection Laws. In this context and for the purposes of the Applicable Data Protection Laws, Customer is the data Controller and SpotQA is the data Processor; and for the purposes of the CCPA (to the extent applicable), Customer is the Business and SpotQA is the Service Provider.

2.2. SpotQA shall process Customer's Personal Data as part of providing Customer with the Services, pursuant to the specifications and for the duration under the Customer Agreement (the "**Term**").

3. Customer Responsibilities

3.1. Within the scope of the Customer Agreement and Customer's use of the Services, Customer will be responsible for complying with all requirements that apply to it under Applicable Data Protection Laws with respect to its Processing of Personal Data. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Without limitation, Customer will provide all necessary notices to relevant Data Subjects, including a description of the Services, and secure all necessary permissions and consents, or other applicable lawful grounds for processing Personal Data pursuant to this DPA. SpotQA shall amend, correct or erase Customer's Personal Data at Customer's request.

3.2. Customer shall be responsible for ensuring that its instructions to SpotQA regarding the Processing of Customer Personal Data comply with applicable laws, including Applicable Data Protection Laws. The parties agree that the Customer Agreement (including this DPA), together with Customer's use of the Services in accordance with the Customer Agreement, constitute the complete instructions to SpotQA in relation to SpotQA's Processing of Customer Personal Data, so long as Customer may provide additional instructions during the Term that are consistent with the Customer Agreement and the nature and lawful use of the Services. Customer will inform SpotQA without undue delay if it is not able to comply with its responsibilities under this section 3 or Applicable Data Protection Laws.

4. SpotQA Obligations as Processor

4.1. SpotQA will only Process Customer Personal Data for the purposes described in this DPA and the Customer Agreement or as otherwise agreed within the scope of Customer's lawful documented instructions, except where and to the extent otherwise required by applicable law.

4.2. If SpotQA becomes aware that it cannot Process Customer Personal Data in accordance with Customer's instructions due to a legal requirement under any applicable law, (i) SpotQA will promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and (ii) SpotQA may, where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Customer Personal Data) and/or suspend access to Customer's account until such time as Customer issues new instructions with which SpotQA is able to comply. If this provision is invoked, SpotQA will not be liable to Customer under the Customer Agreement for any failure to perform the applicable Services until such time as Customer issues new lawful Instructions with regard to the Processing. If the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Customer Agreement and this DPA with respect to the affected processing. Customer will have no further claims against SpotQA (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Customer Agreement and the DPA as described in this paragraph.

4.3. SpotQA will implement and maintain appropriate technical and organisational measures to protect Customer Personal Data from Personal Data Breaches, as described under Appendix A ("**Security Measures**"). Notwithstanding any provision to the contrary, SpotQA may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

4.4. In addition to the confidentiality provisions of the Customer Agreement, SpotQA will ensure that SpotQA's employees, subcontractors or other authorised personnel ("**Authorised Persons**") that process Personal Data are subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Customer Personal Data who is not under such a duty of confidentiality. SpotQA shall ensure that all Authorised Persons process the Customer Personal Data only as necessary for the purposes described in the Customer Agreement and SpotQA shall be fully liable for the actions of such Authorised Persons.

4.5. SpotQA will notify Customer without undue delay after it becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Customer. At Customer's request, SpotQA will promptly provide Customer with such reasonable assistance as necessary to enable Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if it is required to do so under Applicable Data Protection Laws.

4.6. SpotQA acknowledges and confirms that it does not receive or process any Personal Data as consideration for any services or other items that SpotQA provides to Customer under the Customer Agreement. SpotQA shall not have, derive, or exercise any rights or benefits regarding Personal Data Processed on Customer's behalf, and may use and disclose Personal Data solely for the purposes for which such Personal Data was provided to it, as stipulated in the Customer Agreement and this DPA. SpotQA certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Data Processed hereunder, without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Data to or from SpotQA under the Agreement or this DPA to qualify as "selling" such Personal Data under the CCPA.

5. Sub-Processors

5.1. SpotQA may hire Sub-processors to provide certain limited or ancillary services on its behalf. Customer authorises SpotQA's engagement of Sub-processors. Where the Controller to Processor SCCs apply, the Parties agree to use "Option 2" in clause 9 of the Controller to Processor SCCs (i.e., Customer's general written authorisation for the engagement of Sub-processors). SpotQA makes available information about Sub-processors on its Sub-processor Page.

5.2. From time to time, SpotQA may engage new Sub-processors to process personal data on its behalf. SpotQA will give the Customer notice (by updating the website or providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor in advance of engaging that new Sub-processor. Customer may object to the processing of Customer's Personal Data by the new Sub-processor, on reasonable and explained grounds, by providing a written objection to notices@virtuosoqa.com within 5 business days following SpotQA's notice to Customer of the intended engagement with the new Sub-processor. If Customer timely sends SpotQA a written objection notice, the parties will use good-faith efforts to resolve Customer's objection. In the absence of a resolution, SpotQA will use commercially reasonable efforts to provide Customer with the same level of service without using the new Sub-processor to process Customer's Personal Data.

5.3. In the event that SpotQA engages a Sub-processor to assist with or carry the processing activity on its behalf, SpotQA represents and warrants that the processing activity is carried out with at least the

same level of protection for the Customer Personal Data and the rights of Data Subjects as required in the Customer Agreement and this DPA and that at a minimum the same data protection, security, and confidentiality obligations and as set out in this DPA and Customer Agreement shall be imposed on the Sub-processor. Where the Sub-processor fails to fulfil its data protection obligations, SpotQA shall remain fully liable to Customer for the performance of the Sub-processor's obligations.

6. Transfers

6.1. Customer acknowledges and agrees that SpotQA may access and Process Customer Personal Data on a global basis as necessary to provide the Services in accordance with the Customer Agreement, and in particular that Customer Personal Data may be transferred to and Processed by jurisdictions where SpotQA Affiliates and Sub-processors have operations. Wherever Customer Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws.

6.2. Where the transfer of Customer Personal Data between the parties involves a Restricted Transfer and Applicable Data Protection Laws require putting in place appropriate safeguards, SpotQA and Customer will comply with the following:

6.2.1. EEA Restricted Transfers. To the extent that any Processing of Customer Personal Data under this DPA involves an EEA Restricted Transfer from Customer to SpotQA, the Parties agree to enter into the Controller to Processor SCCs, which are hereby deemed to be: (a) populated in accordance with Appendix B; and (b) entered into by the Parties and incorporated by reference into this DPA.

6.2.2. UK Restricted Transfers. To the extent that any Processing of Customer Personal Data under this DPA involves a UK Restricted Transfer from Customer to SpotQA, the Parties agree to enter into the UK Addendum as set out in Appendix C, which is hereby deemed to be entered into by the Parties and incorporated by reference into this DPA.

6.2.3. Swiss Restricted Transfers. To the extent that any Processing of Customer Personal Data under this DPA involves a Swiss Restricted Transfer from Customer to SpotQA, the Parties shall enter into the Controller to Processor SCCs, which are hereby deemed to be: (a) varied to address the requirements of the FADP and populated in accordance with Appendix B; and (b) entered into by the Parties and incorporated by reference into this DPA.

6.3. If and to the extent the SCCs conflict with any provision of this DPA, the SCCs will prevail to the extent of such conflict. If SpotQA cannot comply with its obligations under the SCCs for any reason, and Customer intends to suspend or terminate the transfer of Personal Data to SpotQA, Customer agrees to provide SpotQA with reasonable notice to enable SpotQA to cure such non-compliance and to reasonably cooperate with SpotQA to identify what additional safeguards, if any, may be implemented to remedy such noncompliance. If SpotQA has not or cannot cure the non-compliance, Customer may suspend or terminate the affected part of the Services in accordance with the Customer Agreement without liability to either Party (but without prejudice to any fees incurred prior to such suspension or termination).

6.4. SpotQA may on notice vary this DPA and replace the relevant SCCs with: (a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data

protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or another transfer mechanism, other than the SCCs, that enables the lawful transfer of Customer Personal Data to SpotQA under this DPA in compliance with Chapter V of the GDPR.

7. Notification

7.1. SpotQA has in place reasonable and appropriate security incident management policies and procedures and will notify Customer without undue delay (and in any event within 48 hours) after becoming aware of a Personal Data Breach.

7.2. SpotQA shall make reasonable efforts to identify the cause of such Personal Data Breach, and take those steps as SpotQA deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach, to the extent that the remediation is within SpotQA's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Authorised Users.

7.3. SpotQA will immediately inform Customer of any legally binding request for disclosure of the Personal Data by a law enforcement or regulatory authority.

8. Deletion and Return of Customer Data

8.1. SpotQA will delete or return all Customer Data, including Customer Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of the Services or upon written request by Customer. This term will not apply where SpotQA is required by applicable law to retain some or all of the Customer Data, or where it has archived Customer Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices.

9. Information Requests and Audit Rights

9.1. SpotQA agrees to keep records of all categories of processing activities and to make available all information reasonably necessary to demonstrate compliance with the obligations laid out in this DPA and the relevant provisions of the Applicable Data Protection Law, and cooperate with and contribute to audits and inspections, whether by Customer, its auditors or an EU regulatory body.

9.2. SpotQA agrees to cooperate with Customer to provide all reasonable and timely assistance to Customer to enable Customer to:

9.2.1. comply with any obligations under Applicable Data Protection Law including in particular those set out in Articles 32 to 36 of the GDPR;

9.2.2. conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority;

9.2.3. respond to any request from a Data Subject to exercise rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) and SpotQA agrees to promptly inform Customer if such a request is received directly; and

9.2.4. respond to and comply with any investigations, complaints or requests for information by a Data Subject or person or regulatory, supervisory, or governmental authority in connection with the processing of the Personal Data.

9.3. SpotQA will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and contribute to audits, including inspections conducted by Customer or its auditor in order to assess compliance with this DPA, where required by applicable law. Customer acknowledges that the Services are hosted by SpotQA's hosting Sub-processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that SpotQA's systems are audited annually as part of SOC 2 compliance and regularly tested by independent third-party penetration testing firms. Upon request, SpotQA will supply (on a confidential basis) its SOC 2 report to Customer so that Customer can verify SpotQA's compliance with this DPA.

10. General

10.1. *Amendments*. Notwithstanding anything else to the contrary in the Customer Agreement and without prejudice to section 4.1, SpotQA reserves the right to make any updates and changes to this DPA.

10.2. *Severability*. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

10.3. *Limitation of liability*. The Parties' liability in the aggregate arising out of or in relation to this DPA, whether in contract, tort (including negligence), misrepresentation, or otherwise, shall be subject to any limitation of liability provisions in the Customer Agreement, and, only for the purposes of this DPA, any reference to the liability of a party in those Customer Agreement provisions shall be taken to mean to the liability of that party and its Affiliates.

10.4. *Conflict*. Except as specifically set forth in this DPA, all of the terms and provisions of the Customer Agreement shall remain unmodified and in full force and effect. In the event of any conflict between the Customer Agreement and this DPA, the terms of this DPA will prevail.

10.5. *Governing Law*. This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales, unless required otherwise by Applicable Data Protection Laws.

APPENDIX A: SECURITY MEASURES

("Platform" – https://app.virtuoso.qa)

SpotQA has implemented and will maintain for Customer Personal Data the following security measures, which in conjunction with the security commitments in this DPA, are SpotQA's only responsibility with respect to the security of that data.

SPECIFIC TECHNICAL AND ORGANISATIONAL SECURITY SAFEGUARDS

1. The following specific safeguards are made for SpotQA's technical security:

a) The Platform enforces user authentication at the application level through secure user/password combinations, supplemented by multi-factor authentication (MFA) where applicable.

b) Regular monitoring for vulnerabilities and any discovered vulnerabilities to be promptly addressed within defined time frames based on their severity, following a risk-based approach.

c) Encryption of Customer Data while at rest and in transit consistent with industry standards and at a minimum of 256-bit encryption.

e) Data redundancy and recovery plans, including at least daily backups of Customer Data, ensure timely recovery of the Platform in the event of a major incident.

f) SpotQA maintains network security with industry-standard techniques, including firewalls, intrusion detection, and prevention systems.

g) SpotQA uses the latest antivirus and malware protection software across all relevant systems, with regular monitoring and scanning to detect potential threats. Exceptions, where installing antivirus software may impact operation, performance or productivity, rely on inherent security measures that are designed to effectively prevent malware infections. This is monitored and maintained to ensure equivalent security effectiveness.

h) All Platform activity (including database activity) is logged for accountability,

i) Record and retain audit-logging information for all systems that handle confidential information, accept network connections, or make access control (authentication and authorisation) decisions.

j) Regularly conduct internal security audits and no less than annual external security assessments and penetration tests of company systems.

k) Maintains a digital record of personal data storage locations and follows a standard procedure for secure data deletion in compliance with applicable retention and deletion policies.

l) Ensures that Sub-processors implement robust technical and organisational measures to meet the requirements of the Applicable Data Protection Law, including data protection principles and security safeguards

2. The following specific safeguards are made for SpotQA’s organisational security:

a) All employees are required to sign a confidentiality agreement when accepting a new hire offer and contractors who access the facilities and/or data required to sign a confidentiality or non-disclosure agreement.

b) All employees, contractors, and third-party users are assigned unique User-IDs and regularly briefed and trained on their information security roles and responsibilities, particularly in relation to their data protection obligations and Applicable Data Protection Law.

c) User administration procedures define user roles and privileges, access granting, changes, and termination, as well as ensuring appropriate segregation of duties and monitoring of activities.

d) Access rights are granted based on the 'least privilege' principle, with periodic reviews conducted to ensure that access remains appropriate for each user's role and responsibilities.

e) Upon termination of any employee/contractor, employee’s/contractor’s access to Customer Data on SpotQA systems will be immediately revoked.

APPENDIX B – STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR) MODULE II

1. **SIGNATURE OF THE SCCs**:
   Where the SCCs apply each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. **MODULE**
   Where the EEA Restricted Transfer is a Controller to Processor transfer, specifically where Customer acts as the Controller and data exporter, and SpotQA acts as Processor and data importer, only the provisions relating to Module II apply to such EEA Restricted Transfer.

3. **POPULATION OF THE BODY OF THE SCCs**
   For each Module of the SCCs, the following applies as and where applicable to that Module and the Clauses thereof:
   a. Clause 7 (Docking Clause) shall apply.
   b. Option 2: General Written Authorisation applies and the minimum time period for the data importer to specifically inform the data exporter in writing of any intended changes to that list in accordance with Clause 9 shall be 30 days;
   c. In Clause 11 of the EU SCCs, the optional language will not apply.
   d. In Clause 17 of the EU SCCs, Option 1 shall apply, and the Parties agree that the EU SCCs shall be governed by the laws of Portugal.
   e. In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of the Republic of Ireland.
   f. To the extent there is any conflict between the EU SCCs and any other terms in this DPA or the Customer Agreement, the provisions of the EU SCCs will prevail.

4. **POPULATION OF ANNEXES TO THE APPENDIX TO THE SCCs**

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s):
Name: The Customer, as set out in the Order Form (on behalf of itself and its Permitted Affiliates)

Address: The Customer's address as set out in the Order Form

Contact person's name, position and contact details: The Customer's contact details, as set out in the Order Form

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the SpotQA Services pursuant to the Customer Agreement

Role (controller/processor): …Controller
…
Data importer(s):

Name: SpotQA Limited trading as 'Virtuoso QA'

Address: International House, 64 Nile Street, London, United Kingdom, N1 7SR

Contact person's name, position and contact details: …Head of Legal, notices@virtuosoqa.com

Activities relevant to the data transferred under these Clauses: … Processing of Personal Data in connection with Customer's use of the Services under the Customer Agreement.

Role (controller/processor): …Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Customer contacts and other end users including its employees, contractors, collaborators and subcontractors.

Categories of personal data transferred

The personal data that is provided to SpotQA and included in email, documents and other data in electronic form in the context of the Services. SpotQA acknowledges that, depending on Customer's use of the Services, Customer may elect to include personal data from any of the following categories in the personal data:

General Personal Data, including any data about an identified or identifiable data subject, except for those mentioned in points b) and c). Examples of such data include, but are not limited to, first name, middle names, last name, title, emails, phone numbers, addresses, IP-addresses, un-hashed cookies, other personal identifiers, birthday, sex.

Authentication data (for example user name/handle, password, security question, audit trail);

Contact information (for example physical addresses, email, phone numbers, social media identifiers);

Internet activity (for example browsing and search history while on the Platform);

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).
On a continuous basis as necessary for SpotQA to meet its obligations in conjunction with the provision of the Services for the term of the Customer Agreement (including this DPA) with Customer.

Nature of the processing

Customer Personal Data will be Processed in accordance with the Customer Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Services provided to Customer; and/or

2. Disclosure in accordance with the Customer Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose(s) of the data transfer and further processing
Customer Personal Data will be processed as necessary to provide the Services pursuant to the Customer Agreement, as further specified in the Order Form, and as further instructed by Customer in its use of the Services.

Period for which Personal Data will be retained

Subject to the 'Deletion or Return of Customer Data' section of this DPA, SpotQA will Process Customer Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Dormant accounts are checked intermittently and where contact cannot be made with the user to confirm their intent to maintain the account, the account is cancelled. Upon such cancellation all data associated with that account will no longer be identifiable to a natural person.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Sub-processors are retained in support of the SaaS products/services provided to data exporters and are contractually bound as to subject matter, nature and duration of the processing similarly in kind as the data importer taking into account the sub-processors specific role.

C. COMPETENT SUPERVISORY AUTHORITY
Identification of the competent supervisory authority/ies in accordance with Clause 13F

If the data exporter is established in an EU Member State*: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.*
If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR)*: the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.*
If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU*: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, will act as competent supervisory authority.*

ANNEX II - SECURITY MEASURES

Annex II to the Appendix to the SCCs is populated as below:

Please refer to Appendix A of the DPA.

ANNEX III – SUB-PROCESSORS

To help SpotQA deliver the Services, we engage Sub-processors to assist with our data processing activities. A list of our Sub-processors and our purpose for engaging them is available at https://virtuosoqa.notion.site/Sub-processors-3696590989a744cf96c3d5f5ec4a5ca9 , which is incorporated into this DPA.

APPENDIX C - International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date	The Start Date for this Addendum shall coincide with the start date of each Customer Agreement between the Parties.	
The Parties	**Exporter (who sends the Restricted Transfer)** The Exporter is the Customer as identified in the Order Form between SpotQA and the Customer	**Importer (who receives the Restricted Transfer)** The Importer is SpotQA Limited trading as 'Virtuoso QA'
Parties' details	Exporters' details are as set forth in the Order Form.	Importer's details are as set forth in the Order Form.
Key Contact	Exporter's details are as set forth in the Order Form.	Importer's details are as set forth in the Order Form.
Signature (if required for the purposes of Section 2)	The Parties agree that their signatures affixed to the Order Form shall serve to legally bind the Parties to this Addendum.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or

	☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

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

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: Parties are as set forth in Annex I.A of the EU SCCs found in Appendix B to the DPA.

Annex 1B: Description of Transfer: is as set forth in Annex I.B. of the EU SCCs found in Appendix B to the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Technical and organisational measures are as set forth in Annex II to the EU SCCs found in Appendix A to the DPA.

Annex III: List of Sub processors (Modules 2 and 3 only): Sub-processors are as set forth in Appendix B of the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party. Clause 18 will apply in the event the Approved Addendum changes in accordance therewith

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 1212, the provisions of Section 15 will apply.

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

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

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

    b. In Clause 2, delete the words:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix

Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

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

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

b its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.