

DATA PROCESSING AGREEMENT FOR QUALTRICS CLOUD SERVICES

Parties:	Qualtrics, LLC (" Qualtrics ")
	[SHL Group Ltd] (" Customer ")
Effective Date:	The date signed by the last party to sign.

Qualtrics	Customer
By (signature):	By (signature): <small>DocuSigned by:</small> <i>Emmy Hackett</i>
Name:	Name: Emmy Hackett <small>FB24F46BEA71411...</small>
Title:	Title: General Counsel
Date:	Date: 23 December 2022

1. DEFINITIONS

- 1.1. "Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to Qualtrics be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.
- 1.2. "Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the processing of Personal Data under the Agreement.
- 1.3. "Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.
- 1.4. "EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 1.5. "EU Standard Contractual Clauses"** means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof as adopted by Qualtrics. To avoid doubt Modules 2 and 3 shall apply as set out in Section 8.3.
- 1.6. "GDPR"** means the General Data Protection Regulation 2016/679.
- 1.7. "New SCC Relevant Transfer"** means a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the EU Standard Contractual Clauses.
- 1.8. "Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is:
- a) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service; or
 - b) supplied to or accessed by Qualtrics or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).
- 1.9. "Personal Data Breach"** means a confirmed:
- a) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data; or
 - b) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.
- 1.10. "Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.
- 1.11. "SAP"** means SAP SE, Qualtrics parent company.
- 1.12. "Schedule"** means the numbered Annex with respect to the EU Standard Contractual Clauses.
- 1.13. "Subprocessor" or "sub-processor"** means Qualtrics Affiliates, SAP, SAP Affiliates and third parties engaged by Qualtrics, Qualtrics' Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.
- 1.14. "Technical and Organizational Measures"** means the technical and organizational measures for the relevant Cloud Service set out in Schedule 2.
- 1.15. "Third Country"** means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Purpose and Application

- 2.1.1.** This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Qualtrics and Customer.
- 2.1.2.** This DPA applies to Personal Data processed by Qualtrics and its Subprocessors in connection with its provision of the Cloud Service.
- 2.1.3.** This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by Qualtrics. Customer shall not store Personal Data in such environments.

2.2. Structure

Schedules 1, 2 and 3 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects (Schedule 1), applicable Technical and Organizational Measures (Schedule 2), and the UK addendum to the EU Standard Contractual Clauses, if applicable (Schedule 3).

2.3. Governance

- 2.3.1. Qualtrics acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA.
- 2.3.2. Customer acts as a single point of contact and shall obtain any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Qualtrics as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where Qualtrics informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service. Customer shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Applicability of the Technical and Organizational Measures

Qualtrics has implemented and will apply the Technical and Organizational Measures. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

3.2. Changes

- 3.2.1. Qualtrics applies the Technical and Organizational Measures to Qualtrics' entire customer base hosted out of the same data center or receiving the same Cloud Service. Qualtrics may change the Technical and Organizational Measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
- 3.2.2. Qualtrics will publish updated versions of the Technical and Organizational Measures at www.qualtrics.com/terms-of-service.

4. QUALTRICS OBLIGATIONS

4.1. Instructions from Customer

Qualtrics will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. Qualtrics will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or Qualtrics otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Qualtrics will immediately notify Customer (email permitted).

4.2. Processing on Legal Requirement

Qualtrics may also process Personal Data where required to do so by applicable law. In such a case, Qualtrics shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, Qualtrics and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Qualtrics and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Cooperation

- 4.4.1. At Customer's request, Qualtrics will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Qualtrics' processing of Personal Data or any Personal Data Breach.
- 4.4.2. If Qualtrics receives a request from a Data Subject in relation to the Personal Data processing hereunder, Qualtrics will promptly notify Customer (where the Data Subject has provided information to identify the Customer) via e-mail and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.
- 4.4.3. In the event of a dispute with a Data Subject as it relates to Qualtrics' processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably co-operate with the aim of resolving the dispute amicably with the Data Subject.
- 4.4.4. Qualtrics shall provide functionality for production systems that supports Customer's ability to correct, delete or anonymize Personal Data from a Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Qualtrics will correct, delete or anonymize any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

4.5. Personal Data Breach Notification

Qualtrics will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Qualtrics may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Qualtrics.

4.6. Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, Qualtrics will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports and certifications). Any additional assistance shall be mutually agreed between the Parties.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval by Customer

During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Qualtrics and Customer will find a reasonable method to allow Customer access to Personal Data.

5.2. Deletion

Before the Subscription Term expires, Customer may use Qualtrics' self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs Qualtrics to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed 6 months) unless applicable law requires retention.

6. CERTIFICATIONS AND AUDITS

6.1. Customer Audit

Customer or its independent third party auditor reasonably acceptable to Qualtrics (which shall not include any third party auditors who are either a competitor of Qualtrics or not suitably qualified or independent) may audit Qualtrics' control environment and security practices relevant to Personal Data processed by Qualtrics only if:

- a) Qualtrics has not provided sufficient evidence of its compliance with the Technical and Organizational Measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or Qualtrics;
- b) a Personal Data Breach has occurred;

- c) an audit is formally requested by Customer's data protection authority; or
- d) provided under mandatory Data Protection Law conferring Customer a direct audit right and provided that Customer shall only audit once in any 12 month period unless mandatory Data Protection Law requires more frequent audits.

6.2. Other Controller Audit

Any other Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Controller and such audit is permitted and coordinated by Customer. Customer shall use all reasonable means to combine audits of multiple other Controllers to avoid multiple audits unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by Qualtrics on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

6.3. Scope of Audit

Customer shall provide at least 60 days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of 3 business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Qualtrics.

6.4. Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by Qualtrics of this DPA, then Qualtrics shall bear its own expenses of an audit. If an audit determines that Qualtrics has breached its obligations under the DPA, Qualtrics will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

Qualtrics is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

- a) Qualtrics or Qualtrics affiliates on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Qualtrics shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;
- b) Qualtrics will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and
- c) Qualtrics' list of Subprocessors in place on the effective date of the Agreement is published by Qualtrics at www.qualtrics.com/subprocessor-list or Qualtrics will make it available to Customer upon request, including the name, address and role of each Subprocessor Qualtrics uses to provide the Cloud Service.

7.2. New Subprocessors

Qualtrics' use of Subprocessors is at its discretion, provided that:

- a) Qualtrics will inform Customer in advance (by email or by posting on the Cloud Service) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and
- b) Customer may object to such changes as set out in Section 7.3.

7.3. Objections to New Subprocessors

- 7.3.1. If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to Qualtrics. Such termination shall take effect at the time determined by the Customer which shall be no later than 30 days from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this 30 day period, Customer is deemed to have accepted the new Subprocessor.
- 7.3.2. Within the 30 day period from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions shall not extend the period for

termination and do not affect Qualtrics' right to use the new Subprocessor(s) after the 30 day period.

- 7.3.3. Any termination under this Section 7.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

7.4. Emergency Replacement

Qualtrics may replace a Subprocessor without advance notice where the reason for the change is outside of Qualtrics' reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Qualtrics will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 7.2 applies accordingly.

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

Qualtrics shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

8.2. Applicability of EU Standard Contractual Clauses

Sections 8.3 to 8.6 apply in respect of a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR or applicable Data Protection Law can be met by entering into the EU Standard Contractual Clauses as may be amended in accordance with applicable Data Protection Law.

8.3. Applicability of EU Standard Contractual Clauses where Qualtrics is not located in a Third Country

Where Qualtrics is not located in a Third Country and acts as a data exporter, Qualtrics has entered into the EU Standard Contractual Clauses with each Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses shall apply to such transfers.

8.4. Applicability of EU Standard Contractual Clauses where Qualtrics is located in a Third Country

- 8.4.1. Where Qualtrics is located in a Third Country, or in a country that otherwise requires use of the EU Standard Contractual Clauses for transfers of Personal Data to that country, Qualtrics and Customer hereby enter into the EU Standard Contractual Clauses with Customer as the data exporter and Qualtrics as the data importer as follows:

- a) Module 2 (Controller to Processor) shall apply where Customer is a Controller; and
 - b) Module 3 (Processor to Processor) shall apply where Customer is a Processor.
- Where Customer acts as Processor under Module 3 (Processor to Processor) of the EU Standard Contractual Clauses, Qualtrics acknowledges that Customer acts as Processor under the instructions of its Controller(s).

Other Controllers or Processors whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into the EU Standard Contractual Clauses with Qualtrics in the same manner as Customer in accordance with Section 8.4.1 above. In such case, Customer enters into the EU Standard Contractual Clauses on behalf of other Controllers or Processors.

- 8.4.2. Where Customer is located in a Third Country and is acting as a data importer under Module 2 or Module 3 of the EU Standard Contractual Clauses and Qualtrics is acting as Customer's sub-processor, the respective data exporter shall have the following third-party beneficiary right:

In the event that Customer has factually disappeared, ceased to exist in law or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Customer by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Qualtrics Service solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs Qualtrics to erase or return the Personal Data.

- 8.4.3. On request from a Data Subject, Customer may make a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Customer and Qualtrics (including the relevant Schedules) available to Data Subjects.

8.5. Applicability of EU Standard Contractual Clauses where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses

Subject to Sections 8.2 to 8.4, where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses, then the EU Standard Contractual Clauses are interpreted as follows:

- 8.5.1. In relation to the Swiss Data Protection Act ("**FDPA**"):
- a) the references to a "Member State" in the EU Standard Contractual Clauses will be deemed to include Switzerland;
 - b) references to the law of the European Union or of a Member State in the EU Standard Contractual Clauses shall be deemed to be a reference to the FDPA;
 - c) the Swiss Federal Data Protection and Information Commissioner will be the sole or, where both the FDPA and the GDPR apply to such transfer, one of the competent data protection authorities, under the EU Standard Contractual Clauses;
 - d) the terms used in the EU Standard Contractual Clauses that are defined in the FDPA will be construed to have the meaning of the FDPA; and
 - e) where the FDPA protects legal entities as data subjects, the EU Standard Contractual Clauses will apply to data relating to identified or identifiable legal entities.
- 8.5.2. In relation to the Data Protection Act 2018 of the United Kingdom ("**UK GDPR**"), from 21 September 2022, the EU Standard Contractual Clauses shall be interpreted and construed in accordance with the 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 UK GDPR on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, and attached at Schedule 3 (the "**Approved Addendum**"). Schedules 1 and 2 set out the information for Part 1, Tables of the Approved Addendum.

8.6. Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the EU Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules, such specifications also apply in relation to the EU Standard Contractual Clauses.

9. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

Schedule 1 Description of the Processing

This Schedule 1 applies to describe the Processing of Personal Data for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

1. Optional Clauses Of The EU Standard Contractual Clauses

- 1.1. Except where applicable Data Protection Law requires a variation to the EU Standard Contractual Clauses then the governing law of the EU Standard Contractual Clauses shall be the laws of Ireland.
- 1.2. The optional Clauses 7 and the option in Clause 11a of the EU Standard Contractual Clauses shall not apply.
- 1.3. Option 2, General Written Authorisation of Clause 9 shall apply in accordance with the notification periods set out in Section 7 of this DPA.

2. LIST OF PARTIES

2.1. Under the EU Standard Contractual Clauses

- 2.1.1. Module 2: Transfer Controller to Processor
Where Qualtrics is located in a Third Country, Customer is the Controller and Qualtrics is the Processor, then Customer is the data exporter and Qualtrics is the data importer.
- 2.1.2. Module 3: Transfer Processor to Processor
Where Qualtrics is located in a Third Country, Customer is a Processor and Qualtrics is a Processor, then Customer is the data exporter and Qualtrics is the data importer.

3. DESCRIPTION OF TRANSFER

3.1. Data Subjects

Unless provided otherwise by the data exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service, transmitted to, made available to, accessed or otherwise processed by the data importer.

3.2. Data Categories

The transferred Personal Data concerns the following categories of data: Customer determines the categories of data and/or data fields which could be transferred per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users transferred or entered into the Cloud Service.

3.3. Special Data Categories (if agreed)

- 3.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("Sensitive Data"). Qualtrics has taken Technical and Organizational Measures as set out in Schedule 2 to ensure a level of security appropriate to protect also Sensitive Data.
- 3.3.2. The transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):
 - a) training of personnel;
 - b) encryption of data in transit and at rest;
 - c) system access logging and general data access logging.
- 3.3.3. In addition, the Cloud Services provide measures for handling of Sensitive Data as described in the Documentation.

3.4. Purposes of the data transfer and further processing; Nature of the processing

- 3.4.1. The transferred Personal Data is subject to the following basic processing activities:
 - a) use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support);
 - b) continuous improvement of service features and functionalities provided as part of the Cloud Service including automation, transaction processing and machine learning;
 - c) provision of professional services;

- d) communication to Authorized Users;
- e) storage of Personal Data in dedicated data centers (multi-tenant architecture);
- f) release, development and upload of any fixes or upgrades to the Cloud Service;
- g) back up and restoration of Personal Data stored in the Cloud Service;
- h) computer processing of Personal Data, including data transmission, data retrieval, data access;
- i) network access to allow Personal Data transfer;
- j) monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database;
- k) security monitoring, network-based intrusion detection support, penetration testing; and
- l) execution of instructions of Customer in accordance with the Agreement.

3.4.2. The purpose of the transfer is to provide and support the Cloud Service. Qualtrics and its Subprocessors may support the Cloud Service data centers remotely. Qualtrics and its Subprocessors provide support when a Customer submits a support ticket as further set out in the Agreement.

3.5. Additional description in respect of the EU Standard Contractual Clauses:

3.5.1. The purpose of the transfer is to provide and support the relevant Cloud Service. Qualtrics and its Subprocessors may provide or support the Cloud Service remotely.

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

In respect of the EU Standard Contractual Clauses, transfers to Subprocessors shall be on the same basis as set out in the DPA.

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

Personal Data will be transferred on an ongoing basis for the duration of the Agreement.

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

Personal Data shall be retained for the duration of the Agreement and subject to Section 5 of the DPA.

4. COMPETENT SUPERVISORY AUTHORITY

4.1. In respect of the EU Standard Contractual Clauses:

4.1.1. Module 2: Transfer Controller to Processor

4.1.2. Module 3: Transfer Processor to Processor

4.2. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Clause 13 of the EU Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and applicable Data Protection Law.

Qualtrics will apply and maintain the Technical and Organizational Measures.

To the extent that the provisioning of the Cloud Service comprises New SCC Relevant Transfers, the Technical and Organizational Measures set out in Schedule 2 describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws may affect the compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define Qualtrics' current technical and organizational measures. Qualtrics may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- Qualtrics protects its assets and facilities using the appropriate means based on the Qualtrics Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Qualtrics buildings must register their names at reception and must be accompanied by authorized Qualtrics personnel.
- Qualtrics employees and external personnel must wear their ID cards at all Qualtrics locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- Qualtrics and all third-party Data Center providers log the names and times of authorized personnel entering Qualtrics' private areas within the Data Centers.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the Qualtrics Security Policy
- All personnel access Qualtrics' systems with a unique identifier (user ID).
- Qualtrics has procedures in place so that requested authorization changes are implemented only in accordance with the Qualtrics Security Policy (for example, no rights

are granted without authorization). In case personnel leaves the company, their access rights are revoked.

- Qualtrics has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Qualtrics uses up-to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant
- security updates. Full remote access to Qualtrics' corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- As part of the Qualtrics Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Qualtrics uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Qualtrics Security Policy.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, Qualtrics conducts internal and external security checks and penetration tests on its IT systems.
- An Qualtrics security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Qualtrics to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over Qualtrics internal networks is protected according to Qualtrics Security Policy.
- When data is transferred between Qualtrics and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Qualtrics-controlled systems (e.g. data being transmitted outside the firewall of the Qualtrics Data Center).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Qualtrics data processing systems.

Measures:

- Qualtrics only allows authorized personnel to access Personal Data as required in the course of their duty.

- Qualtrics has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Qualtrics or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- Qualtrics uses controls and processes to monitor compliance with contracts between Qualtrics and its customers, subprocessors or other service providers.
- As part of the Qualtrics Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Qualtrics Information Classification standard.
- All Qualtrics employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Qualtrics customers and partners.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Qualtrics employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- Qualtrics uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- Qualtrics has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Measures:

- Qualtrics uses the technical capabilities of the deployed software (for example: multi-tenancy, system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

Qualtrics has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, Qualtrics uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

Schedule 3 - International Data Transfer Addendum to the EU Standard Contractual Clauses: Tables

Table 1: Parties

Addendum Effective Date / Start date	<p>Either (a) 21st September 2022, where the effective date of the Agreement is before 21st September 2022; or (b) otherwise, on the effective date of the Agreement.</p> <p>Notwithstanding the Effective Date of this Addendum, Customer acknowledges that Qualtrics will implement the UK Addendum with subprocessors within the time period permitted by applicable law, and at the Effective Date of this Addendum, the UK Addendum may not be in place with subprocessors.</p>	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Customer	Qualtrics
Key Contact	<p>See details in Schedule 1 of the DPA. Customer's Data Protection Officer or other legal representative shall be the key contact. Customer shall make these details available upon Qualtrics' request.</p>	<p>See details in Schedule 1 of the DPA. Qualtrics' Data Protection Officer or other legal representative shall be the key contact. Qualtrics shall make these details available upon Customer's request.</p>

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p>The version of the Approved EU SCCs, which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: Effective Date of the DPA</p> <p>Reference: the EU Standard Contractual Clauses referenced in the DPA</p>
-------------------------	--

Table 3: Appendix Information

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

Annex 1A: List of Parties: See Schedule 1 of the DPA
Annex 1B: Description of Transfer: See Schedule 1 of the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2 of the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p>
--	---

	<input type="checkbox"/> neither Party
--	--