THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

SAN BERNARDINO COUNTY

Contract Number 25-732

SAP Number

Performance, Education and Resource Centers

Department Contract Representative	Julie West
Telephone Number	(909) 387-2462
Contractor	Qualtrics, LLC
Contractor Representative	Caitlin Reader
Telephone Number	(571) 662-3357
Contract Term	October 1, 2025 – September 30, 2026
Original Contract Amount	N/A
Amendment Amount	N/A
Total Contract Amount	N/A
Cost Center	N/A
Grant Number (if applicable)	N/A

Briefly describe the general nature of the contract:

Approve non-financial agreement with Qualtrics, LLC, including nonstandard terms, for a subscription to cloud-based employee experience software and an employee engagement survey system, for the contract period of October 1, 2025 through September 30, 2026.

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
Signed by: Bonnie Uphold	Signed by: Lisa Rivas-Ordaz	Signed by: Victor Tordesillas
Bonnie Uphold, Supervising Deputy County Counsel	Lisa Rivas-Ordaz, Contracts Manager	Victor Tordesillas, Deputy Executive Officer
Date 9/12/2025	Date 9/15/2025	Date 9/12/2025

General Terms and Conditions for Indirect Qualtrics Services ("GTC")

1. Definitions.

1.1 "**Affiliate**" of a party means any legal entity in which such party, directly or indirectly, holds more than 50% of the entity's shares or voting rights, as long as that interest is maintained.

1.2 "**Agreement**" means a EULA Acceptance Form and documents incorporated into a EULA Acceptance Form, including this GTC.

1.3 "**Authorized User**" means any individual that Customer authorizes to use the Cloud Service that is an employee, agent, contractor, or representative of Customer or Customer's Affiliates.

1.4 "**Cloud Service**" means any distinct, subscription-based, hosted, supported, and operated on-demand solution provided by Qualtrics on behalf of Partner to the Customer under a EULA Acceptance Form.

1.5 "**Cloud Materials**" means any materials provided or developed by Qualtrics (independently or with Customer's cooperation) in the course of performance under the Agreement, including Analyses and materials provided or developed in the delivery of any support or Professional Services to Customer. Cloud Materials do not include Customer Data, Customer Confidential Information, or the Cloud Service.

1.6 "**Confidential Information**" means all information that the disclosing party protects against unrestricted disclosure to others that (a) the disclosing party or its representatives designate as confidential, internal, or proprietary at the time of disclosure, or (b) should reasonably be understood to be confidential at the time of disclosure given the nature of the information and the circumstances surrounding its disclosure.

1.7 "**Customer**" means the Customer set forth in the EULA Acceptance Form.

1.8 "**Customer Data**" means any content, materials, data, and information that Authorized Users enter or collect into the production system of the Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g., Customer-specific reports). Customer Data and its derivatives do not include Qualtrics' Confidential Information.

1.9 "**Documentation**" means Qualtrics' then-current technical and functional documentation, including any roles and responsibilities descriptions relating to the Cloud Service, that Qualtrics makes available to Customer under the Agreement.

1.10 "**EULA Acceptance Form**" means the EULA Acceptance Form executed between Qualtrics and the Customer that references these GTCs.

1.11 "**Export Laws**" means all import, export control, and sanctions laws of the United States.

1.12 "**Feedback**" means input, comments, or suggestions regarding Qualtrics' business and technology direction and the possible creation, modification, or improvement of the Cloud Service or Cloud Materials.

1.13 "**Partner**" means entity identified as Partner in the EULA Acceptance Form.

1.14 "**Product Terms**" means the product terms relating to Customer's use of the Cloud Service as set forth in a EULA Acceptance Form.

1.15 "**Professional Services**" means implementation services, consulting services, or other professional services provided under a EULA Acceptance Form.

1.16 "**Qualtrics**" means Qualtrics, LLC, or the affiliate thereof set forth in the Order Form.

1.17 "**Subscription Term**" means the term of the Cloud Service subscription identified in the applicable EULA Acceptance Form, together with all renewals.

1.18 "**Usage Metric**" means the standard of measurement for determining the permitted use for the Cloud Service as set forth in a EULA Acceptance Form.

2. Usage Rights and Restrictions.

2.1 **Grant of Rights.** Subject to Partner's payment of all fees owed to Qualtrics and as set forth in the EULA Acceptance Form, Qualtrics grants to Customer on behalf of Partner a non-exclusive and non-

transferable right to use the Cloud Service, Cloud Materials, and Documentation solely for Customer's and its Affiliates' internal business purposes, including collecting information from third parties for such internal business purposes. Customer may use the Cloud Service worldwide except from countries or regions where such use is prohibited by applicable law (including Export Laws) or as otherwise set forth in the Agreement. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.

2.2 **Authorized Users**. Customer may permit Authorized Users to use the Cloud Service. Customer will not permit an Authorized User's access credentials for the Cloud Service to be used by more than one individual but may permit them to be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

2.3 **Acceptable Use Policy**. Customer will not:

(a) copy, translate, disassemble, decompile, make derivative works of, or reverse engineer the Cloud Service or Cloud Materials (or attempt any of the foregoing);

(b) enter, store, collect, or transfer any content or data on or through the Cloud Service that is unlawful or infringes any intellectual property, privacy, publicity, or other rights;

(c) use the Cloud Service in a way that circumvents Usage Metrics or Product Terms;

(d) access the Cloud Service through unauthorized means (e.g., scraping, crawling, or penetration testing);

(e) circumvent or endanger the operation or security of the Cloud Service; or

(f) remove Qualtrics' copyright and authorship notices from the Cloud Service or Cloud Materials.

2.4 **Verification of Use**. Usage is limited to the Usage Metrics and volumes set forth in the EULA Acceptance Form. Qualtrics may monitor use to the extent necessary to verify compliance with Usage Metrics, volume, and the Agreement and may share any information regarding such compliance or non-compliance with Partner.

2.5 **Suspension of Cloud Service**. Qualtrics may suspend or limit use of the Cloud Service if continued use breaches Section 2.3 or may result in material harm to Qualtrics or the Cloud Service or its users. Qualtrics will promptly notify Customer of the suspension or limitation and will limit a suspension or limitation in time and scope as reasonably possible under the circumstances.

2.6 **Third-Party Web Services**. Through the Cloud Service, Customer may access integrations with third-party services that are subject to terms and conditions with those third parties. These third-party services are not part of the Cloud Service, and the Agreement does not apply to them.

3. Qualtrics Responsibilities.

3.1 **Provisioning**. Qualtrics provides access to the Cloud Service as described in the Agreement.

3.2 **Support**. Qualtrics provides support for the Cloud Service as referenced in the EULA Acceptance Form or the Documentation.

3.3 **Security**. Qualtrics will implement and maintain technical and organizational measures to protect the personal data processed by Qualtrics as part of the Cloud Service as described in the Data Processing Agreement attached hereto as Exhibit A ("**DPA**").

3.4 **Analyses**. Qualtrics or Qualtrics' Affiliates may create analyses by using anonymized and aggregated information related to Customer's use of the Cloud Service ("**Analyses**"). Analyses will not include any personal data.

4. Customer and Personal Data.

4.1 **Customer Data**. As between the parties, Customer is responsible for the content and accuracy of the Customer Data.

4.2 **Personal Data.** Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data protection and privacy laws.

4.3 **Security.** Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct, facilitate, or authorize penetration tests of the Cloud Service without Qualtrics' prior written consent.

4.4 **Access to Customer Data.**

(a) During the Subscription Term, Customer may access Customer Data at any time and may export Customer Data in a standard format. If Customer is unable to export Customer Data, then upon Customer's request, Qualtrics and Customer will find an alternative reasonable method to allow Customer access to Customer Data, which may include Qualtrics delivering an export to Customer.

(b) After the end of the Subscription Term, Qualtrics will delete all Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.

(c) If Customer requires Qualtrics' assistance in connection with third-party legal proceedings relating to the Customer Data, Qualtrics will cooperate with Customer in compliance with applicable law (at Customer's expense) with respect to handling of the Customer Data.

5. Partner Relationship.

5.1 **Non-Payment by Partner.** Qualtrics may suspend Customer's use of the applicable Cloud Service or terminate the Agreement if Partner fails to pay any fee or other amount payable by it on its due date.

5.2 **Termination of Partner Relationship or Orders Relating to Customer.** If (1) Partner terminates all orders relating to the Customer; (2) Qualtrics terminates any of Partner's orders relating to the Customer for good cause, or (3) the partnership between Qualtrics and Partner relating to the sale of subscriptions for the Cloud Service is terminated, Qualtrics may (depending on Customer's choice):

(a) directly provide the affected Cloud Service to the Customer pursuant to Qualtrics' then-current General Terms and Conditions for Qualtrics Services for mutually-agreed subscription fees; or

(b) recommend to Customer other partners or third parties for the provision of the affected Cloud Service.

5.3 **Independence of Partner.** Partner is not an agent of Qualtrics. It is an independent entity with no authority to bind Qualtrics or to make representations or warranties on Qualtrics' behalf. Qualtrics will not be liable for reasonably relying on the accuracy and reliability of written information provided by Partner in making any decision that would give Qualtrics reason to suspend the Cloud Service or terminate the Agreement.

5.4 **No Representation or Warranties.** Qualtrics makes no representations or warranties as to any distributor or reseller, or any other third party, related to the delivery of the products or performance of the services by such entities, and fully disclaims any such warranties in accordance with Section 7.

6. Term and Termination.

6.1 **Term.** The Subscription Term is as set forth in the EULA Acceptance Form.

6.2 **Termination.**

(a) A party may terminate the Agreement:

(1) upon 30 days' prior written notice if the other party materially breaches the Agreement (including Customer's failure to pay Partner any fees due for the Cloud Service) unless the breach is cured during that 30-day period,

(2) as permitted under any other section herein (with termination effective 30 days after receipt of notice in each of these cases unless a different period is specified), or

(3) immediately if the other party files for bankruptcy, becomes insolvent, makes an assignment for the benefit of creditors, or materially breaches Section 11, 12.4, or 12.6.

(b) Qualtrics may terminate the Agreement if the Cloud Service is terminated between Qualtrics and Partner.

6.3 Refund and Payments. For termination by Customer or an 8.1(c) termination by Qualtrics, Customer will be entitled to:

(a) a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective termination date, and

(b) a release from the obligation to pay fees due for periods after the effective termination date.

6.4 Effect of Expiration or Termination. Upon the effective termination or expiration date of the Agreement, Customer's right to use the Cloud Service and all Qualtrics Confidential Information will end.

6.5 Survival. Sections 1, 5, 6.3, 6.4, 6.5, 7.5, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

7. Warranties.

7.1 Compliance with Law. Customer warrants its current and continuing compliance with all laws and regulations applicable to it in connection with the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices. Qualtrics will provide the Cloud Service:

(a) in substantial conformance with the Documentation; and

(b) with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service.

7.3 System Availability.

(a) Qualtrics warrants to maintain an average monthly system availability for the production system of the Cloud Service as set forth in the service level agreement at https://www.qualtrics.com/legal/customers/service-level-agreement ("**SLA**"). Any modification to the SLA by Qualtrics after the effective date of this GTC will not apply. For Customer's records, Customer may download the SLA as of the effective date of this GTC.

(b) Customer's sole and exclusive remedy for Qualtrics' breach of the SLA is the issuance of a credit in the amount described in the SLA, whereby the service level credit will be calculated based on the undiscounted subscription fee set forth in the order form between Qualtrics and Partner. Customer will promptly notify Partner in writing (email permitted) after discovery that Qualtrics does not meet the SLAs. When Qualtrics confirms the validity of the service credit to Partner, Qualtrics will issue such credit to Partner who is then responsible for forwarding the credit to Customer.

7.4 Warranty Exclusions. The warranties in Sections 7.2 and 7.3 will not apply if:

(a) the Cloud Service is not used in accordance with the Agreement or Documentation,

(b) any non-conformity is caused by Partner or Customer or by any product or service not provided by Qualtrics, or

(c) the Cloud Service was provided for no fee.

7.5 Disclaimer. Except as expressly set forth in the Agreement, Qualtrics makes no representations or warranties, express or implied, statutory or otherwise, regarding any matter, including non-infringement or merchantability, suitability, originality, or fitness for a particular use or purpose. Customer acknowledges that it is not relying on delivery of future functionality, public comments, advertising of Qualtrics, or product roadmaps in obtaining any Cloud Service.

8. Third-Party Claims.

8.1 Claims Brought Against Customer.

(a) Qualtrics will defend and indemnify (as set forth in the next sentence) Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's or its Affiliates' use of the Cloud Service infringes or misappropriates a patent claim, copyright, or trade secret right. Qualtrics will indemnify Customer against all damages and costs awarded against Customer and its Affiliates (or the amount of any settlement Qualtrics enters into) with respect to these claims.

(b) Qualtrics' obligations under Section 8.1 will not apply if the claim results from (1) use of the Cloud Service not permitted under the Agreement, (2) use of the Cloud Service in conjunction with any product or service not provided by Qualtrics, or (3) use of the Cloud Service provided for no fee.

(c) If a third party makes a claim of intellectual property infringement or misappropriation covered in Section 8.1, or in Qualtrics' reasonable opinion is likely to make such a claim, Qualtrics may at its expense (1) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (2) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, Qualtrics may terminate Customer's subscription to the affected Cloud Service upon written notice.

8.2 Claims Brought Against Qualtrics. Customer will defend and indemnify (as set forth in the next sentence) Qualtrics against claims brought against Qualtrics and its Affiliates and subcontractors by any third party related to Customer Data. Customer will indemnify Qualtrics against all damages and costs awarded against Qualtrics and its Affiliates and subcontractors (or the amount of any settlement Customer enters into) with respect to these claims.

8.3 Third-Party Claim Procedure. All third-party claims under Section 8 will be conducted as follows:

(a) the party against whom a third-party claim is brought (the "**Indemnified Party**") will timely notify the other party (the "**Indemnifying Party**") in writing of any claim and will reasonably cooperate in the defense of such claim;

(b) the Indemnifying Party will fully control the defense;

(c) subject to Section 8.3(b), the Indemnified Party may appear (at its own expense) through counsel reasonably acceptable to the Indemnifying Party;

(d) any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the Indemnified Party; and

(e) the Indemnifying Party's obligations will not apply if the Indemnified Party's failure to timely notify the Indemnifying Party in writing of any such claim prejudices the Indemnifying Party.

8.4 Exclusive Remedy. The provisions of Section 8 state the sole, exclusive, and entire liability of the parties and their Affiliates and subcontractors to the other party, and is the other party's sole remedy, with respect to covered third-party claims and to the infringement or misappropriation of third-party intellectual property rights.

9. Limitation of Liability.

9.1 Unlimited Liability. Neither party's liability is limited with respect to:

(a) the parties' obligations under Section 8.1(a) and 8.2,

(b) death or bodily injury arising from either party's gross negligence or willful misconduct, or

(c) Customer's failure to pay any fees due under the Agreement.

9.2 Liability Cap. Subject to Section 9.1, the maximum aggregate liability of either party (or its respective Affiliates or Qualtrics' subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any 12-month period will not exceed the annual fees paid by Partner to Qualtrics for the applicable Cloud Service or Professional Service associated with the damages for that

12-month period. Any "12-month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3 **Exclusion of Damages**. Subject to Section 9.1, in no case will either party (or its respective Affiliates or Qualtrics' subcontractors) be liable to the other party for any special, incidental, consequential, or indirect damages, loss of goodwill or business profits, work stoppage, or for exemplary or punitive damages.

10. Intellectual Property Rights.

10.1 **Qualtrics Ownership**. Except for any rights expressly granted to Customer under the Agreement, Qualtrics or Qualtrics' Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Professional Services, design contributions, related knowledge or processes, and any derivative works of them.

10.2 **Customer Ownership**. Customer retains all rights in and related to the Customer Data.

11. Confidentiality.

11.1 **Use of Confidential Information**.

(a) The receiving party will:

(1) maintain the confidentiality of the disclosing party's Confidential Information, taking steps to protect such Confidential Information that are at least as protective of the Confidential Information as those steps that the receiving party takes to protect its own Confidential Information, which will not be less than a reasonable standard of care;

(2) not disclose the disclosing party's Confidential Information to any person other than its Affiliates, employees, contractors, agents, legal representatives, accountants, or other professional advisors, in each case whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality no less onerous than those in this Section;

(3) not use or reproduce the disclosing party's Confidential Information for any purpose outside the scope of the Agreement; and

(4) retain any confidential, internal, or proprietary notices or legends that appear on the original and on any reproductions.

(b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to this Section.

(c) The receiving party may disclose the disclosing party's Confidential Information to the extent required by law, regulation, court order, or regulatory agency if the receiving party uses reasonable efforts to give the disclosing party reasonable prior notice of such required disclosure (to the extent legally permitted) and provides reasonable assistance in contesting the required disclosure, at the request and cost of the disclosing party. The receiving party will use commercially reasonable efforts to disclose only that portion of the Confidential Information that is legally required to be disclosed and will request that all Confidential Information that is so disclosed be accorded confidential treatment.

11.2 **Exceptions**. The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:

(a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,

(b) has become generally known or available to the public through no act or omission by the receiving party,

(c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions,

(d) is lawfully acquired free of restriction by the receiving party from a third party having the right to furnish such Confidential Information, or

(e) the disclosing party agrees in writing is free of confidentiality restrictions.

11.3 Destruction of Confidential Information. Upon the disclosing party's request, the receiving party will promptly destroy or return the disclosing party's Confidential Information, including copies and reproductions thereof. The return and deletion of Customer Data is separately addressed in Section 4.4. The obligation to destroy or return Confidential Information will not apply:

(a) to Confidential Information that the receiving party is legally required to retain, including because legal proceedings related to the Confidential Information prohibit its return or destruction, until the proceedings are settled or a final judgment is rendered; or

(b) to Confidential Information held in archive or back-up systems under general systems archiving or backup policies.

12. Miscellaneous.

12.1 Severability. If any provision of the Agreement is held to be wholly or in part invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

12.2 No Waiver; Amendment. A waiver of any breach of the Agreement is not deemed a waiver of any other breach. The Agreement may be modified solely in writing signed by both parties.

12.3 Counterparts. The Agreement may be signed in counterparts, each of which is an original and together constitute one Agreement. Electronic signatures that comply with applicable law are deemed original signatures.

12.4 Trade Compliance.

(a) Qualtrics and Customer will comply with Export Laws in the performance of the Agreement, with Customer being responsible for obtaining any export authorizations required for sharing Customer Data.

(b) Customer is not (and will not use or permit use of the Cloud Service in connection with any person that is):

(1) located, organized, or resident in Belarus, Cuba, Iran, North Korea, Russia, Syria, the Crimea, the Donetsk People's Republic (DNR) or Luhansk People's Republic (LNR) regions of Ukraine, or any country or region that is subject to comprehensive economic sanctions, or

(2) a designated, denied, or otherwise restricted party under Export Laws.

12.5 Notices. All notices will be in writing and deemed given when delivered, (a) for Qualtrics, to notice@qualtrics.com with a physical copy to Qualtrics, Attn: Legal, 333 W River Park Dr, Provo UT 84604, USA, or, (b) for Customer, to the email or physical address set forth in a EULA Acceptance Form or Agreement or by an electronic notice to Customer's authorized representative or administrator. Qualtrics may provide system notifications and information relating to the operation, hosting, or support of the Cloud Service within the Cloud Service or make such notifications available through the Qualtrics support portal. Customer will maintain up-to-date notice contact information within the Cloud Service.

12.6 Assignment. Without Qualtrics' prior written consent, Customer will not assign, delegate, or transfer the Agreement (or any of its rights or obligations) to any party. Qualtrics may assign the Agreement to Qualtrics' Affiliates.

12.7 Subcontracting. Qualtrics may subcontract parts of the Cloud Service or Professional Services to third parties. Qualtrics is responsible for its subcontractors' performance under the Agreement to the same extent it is responsible for its own performance.

12.8 **Relationship of the Parties**. The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties is created by the Agreement.

12.9 **Force Majeure**. Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. For such a delay, the time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 **Governing Law and Disputes**. The Agreement and any claims arising out of or in connection with the Agreement and its subject matter will be governed by and construed under the laws of the State of Delaware, without reference to its conflicts of law principles. The parties submit to the exclusive jurisdiction of, and the exclusive venue for any disputes arising under the Agreement will be in, the courts located in Wilmington, Delaware. Each party waives any right it may have to a jury trial for any claim or cause of action relating to the Agreement. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act (where enacted) will not apply to the Agreement.

12.11 **Entire Agreement**. The Agreement constitutes the complete and exclusive statement of the agreement between Qualtrics and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. Terms and conditions of any Customer-issued purchase order will have no force and effect.

12.12 **Feedback**. Customer may in its sole discretion provide Qualtrics with Feedback, in which case Qualtrics and its Affiliates may retain and freely use such Feedback without restriction, compensation, or attribution to the source of the Feedback. Customer is not responsible for Qualtrics' use of any Feedback.

Exhibit A
Data Processing Agreement ("DPA")

Personal Data Processing Agreement for Qualtrics Services

1. Definitions.

1.1 "**Controller**" means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For the purposes of this DPA, if Customer acts as processor for another controller, Customer will, in relation to Qualtrics, be deemed as an additional and independent Controller with the controller rights and obligations under this DPA.

1.2 "**Customer Instructions**" means Customer's documented processing instructions (a) as set forth in the Agreement; (b) as reflected by Customer's use of the Cloud Service; and (c) as otherwise reasonably provided to Qualtrics.

1.3 "**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.

1.4 "**Data Subject**" means an identified or identifiable natural person as defined by Data Protection Law.

1.5 "**Permitted Controllers**" means any other Controller authorized by Customer under the Agreement.

1.6 "**Personal Data**" means any information relating to a Data Subject that is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data that 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 to provide support under the Agreement. Personal Data is a subset of Customer Data (as defined under the Agreement).

1.7 "**Personal Data Breach**" means a breach of security that leads to a confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized third-party access to 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.

1.8 "**Processor**" means a natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Controller.

1.9 "**Subprocessor**" means any third party authorized by Qualtrics to process Personal Data in accordance with this DPA.

1.10 "**Technical and Organizational Measures**" means the technical and organizational measures set forth in Schedule 2 for the Cloud Service.

2. Background.

2.1 Purpose and Application.

(a) This DPA is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Qualtrics and Customer.

(b) This DPA applies to Personal Data processed by Qualtrics and its Subprocessors in connection with its provision of the Cloud Service.

(c) This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by Qualtrics. Qualtrics will only provide Customer with access to a non-production environment on request and will clearly indicate that such environment is a non-production environment. Customer will not store Personal Data in such environments.

(d) The subject matter and details of the processing of Personal Data are described in Schedule 1.

2.2 **Governance**.

(a) Qualtrics acts as a Processor, and Customer and Permitted Controllers act as Controllers under the DPA.

(b) Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Qualtrics to lawfully process Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects. Customer acts as a single point of contact for Permitted Controllers in accordance with this DPA. If Customer provides authorizations, consent, instructions, or permissions, these are also provided on behalf of any Permitted Controllers. If Qualtrics informs or gives notice to Customer, such information or notice is deemed received by Permitted Controllers, and Customer will forward such information and notices to the relevant Permitted 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 acknowledges that, as to the Cloud Service selected by Customer in the EULA Acceptance Form, the measures are appropriate taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of Personal Data.

3.2 **Changes**. 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. Qualtrics will publish updated versions of the Technical and Organizational Measures at www.qualtrics.com/legal/customers/gtcs/.

4. **Qualtrics Obligations.**

4.1 **Instructions from Customer**. Qualtrics will process Personal Data only in accordance with (a) Customer Instructions or (b) Section 4.2. For any Customer Instructions not made in the Agreement (including this DPA) or through Customer's use of the Cloud Service, Qualtrics will use reasonable efforts to follow such instructions to the extent they are required by Data Protection Law, technically feasible, and do not require changes to the Cloud Service. If Qualtrics 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 if required to do so by applicable law, in which case Qualtrics will notify Customer of that legal requirement before processing unless that law prohibits such notification.

4.3 **Personnel**. To process Personal Data, Qualtrics and its Subprocessors will 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**.

(a) At Customer's request, Qualtrics will reasonably cooperate with Customer and Permitted Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Qualtrics' processing of Personal Data or any Personal Data Breach.

(b) If Qualtrics receives a request from a Data Subject in relation to Personal Data, Qualtrics will promptly notify Customer (if the Data Subject has provided information to identify Customer and if such notification is permitted by applicable law) by email and will not respond to such request itself but instead ask the Data Subject to redirect its request to Customer.

(c) In the event of a dispute with a Data Subject related to Qualtrics' processing of Personal Data, the parties will keep each other informed and, if appropriate, reasonably cooperate with the aim of resolving the dispute amicably with the Data Subject.

(d) Qualtrics will provide functionality that supports Customer's ability to correct, delete, or anonymize Personal Data within a Cloud Service, or to restrict its processing in line with Data Protection Law. If such functionality is not provided, Qualtrics will assist Customer to 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 in meeting its obligations to report a Personal Data Breach as required under Data Protection Law. Qualtrics may provide such information in phases as it becomes available. Except to the extent required by applicable law, neither party will notify any third party or make any public announcement regarding an incident involving Personal Data or any Personal Data Breach in a manner that would identify the other party without the other party's written consent (not to be unreasonably withheld).

4.6 **Data Protection Impact Assessment**. If Data Protection Law requires Customer or Permitted Controllers to perform a data protection impact assessment or prior consultation with a regulator, then, at Customer's request, Qualtrics will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, and audit reports and certifications). The parties, acting reasonably and in good faith, will agree on any additional assistance.

5. Data Export and Deletion.

5.1 **Export by Customer**. During the Subscription Term and subject to the Agreement, Customer may access Personal Data at any time and may export Personal Data in a standard format (such export constituting a "return" of Personal Data). If Customer is unable to export Personal Data, then upon Customer's request, Qualtrics and Customer will find an alternative reasonable method to allow Customer access to Personal Data, which may include Qualtrics delivering an export to Customer.

5.2 **Deletion**. At the end of the Subscription Term, Customer hereby instructs Qualtrics to delete all Personal Data remaining on servers hosting the Cloud Service within a reasonable time in line with Data Protection Law (not to exceed six 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 will not include any third-party auditors who are either a competitor of Qualtrics or not suitably qualified) may audit Qualtrics' control environment and security practices relevant to Personal Data only if:

(a) Qualtrics has not provided sufficient evidence of its compliance with the Technical and Organizational Measures through providing either: (1) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (2) a valid SOC1-3 attestation report;

(b) the audit is in response to the occurrence of a Personal Data Breach;

(c) the audit is formally requested by Customer's data protection authority; or

(d) Data Protection Law grants Customer a direct audit right, in which case Customer will only audit once in any 12-month period unless Data Protection Law requires more frequent audits.

6.2 **Permitted Controller Audit**. Any Permitted Controller may assume Customer's rights under Section 6.1 only if it applies directly to the Permitted Controller and such audit is permitted and coordinated by Customer. Customer will use all reasonable means to combine audits of all Permitted Controllers to

avoid multiple audits unless Data Protection Law requires the audit to be undertaken by the Permitted Controller itself.

6.3 **Scope of Audit**. Customer will provide at least 60 days' advance notice of any audit unless Data Protection Law or a competent data protection authority requires shorter notice. The parties, acting reasonably and in good faith, will agree on the frequency and scope of any audits. Customer audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer will provide the results of any audit to Qualtrics and, to the extent permitted by applicable law, treat such results as Qualtrics' Confidential Information.

6.4 **Cost of Audits**. Customer will bear the costs of any audit unless such audit reveals a material breach by Qualtrics of this DPA, in which case Qualtrics will bear its own costs. 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**.

(a) Qualtrics is granted a general authorization to subcontract the processing of Personal Data to Subprocessors.

(b) Qualtrics, or Qualtrics affiliates on its behalf, will engage Subprocessors under a written agreement consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Qualtrics is responsible for the Subprocessor's performance under the Agreement to the same extent it is responsible for its own performance.

(c) Qualtrics will evaluate the security, privacy, and confidentiality practices of a Subprocessor prior to selection to establish that it can provide the level of protection of Personal Data required by this DPA.

(d) 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.

7.2 **New Subprocessors; Objections.**

(a) Qualtrics will inform Customer in advance (by email, the support portal, Documentation, or the Cloud Service) of any intended additions or replacements to the list of Subprocessors, including the name, address, and role of the new Subprocessor.

(b) If Customer objects to the new Subprocessor's processing of Personal Data based on reasonable data protection concerns, Customer may terminate its subscription to the affected Cloud Service on written notice to Qualtrics. Such termination will take effect at the time determined by Customer, but no later than 30 days after the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this period, Customer is deemed to have accepted the new Subprocessor.

(c) Within the 30-day period after the date of Qualtrics' notice to Customer of the new Subprocessor, Customer may request that the parties discuss in good faith a resolution to the objection. Such discussions will not extend the period for termination and do not affect Qualtrics' right to use the new Subprocessor after the 30-day period.

(d) Any termination under this Section will be deemed to be without fault by either party and will be subject to the terms of the Agreement.

7.3 **Emergency Replacement**. Qualtrics may replace a Subprocessor without the advance notice set forth in this Section if the reason for the change is outside of Qualtrics' reasonable control and prompt replacement is required for security or other urgent reasons. Qualtrics will inform Customer of the replacement Subprocessor as soon as possible, and the above objection and termination rights apply accordingly.

8. **Processing Locations.**

8.1 **Cross-Border Data Transfers.** Qualtrics may process Personal Data, including by using Subprocessors, outside the data center region selected by Customer as necessary to provide and support the Cloud Service. If processing hereunder results in a Restricted Transfer (as defined in Schedule 3), then the applicable terms in Schedule 3 will apply.

8.2 **Region-Specific Terms.** If Customer believes that Data Protection Law requires specific data protection terms that are not included herein (e.g., due to the location of Customer's operations), Customer will notify Qualtrics, and Qualtrics will propose the appropriate terms to include in an amendment to this DPA (e.g., as a new Schedule 4) or will provide a reasonable explanation for why such terms are not required.

9. **Documentation; Records of Processing.** Each party is responsible for complying with any obligation it has under Data Protection Law to maintain records of processing. Each party will reasonably assist the other party to enable the other party to comply with such obligation, including by providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system).

Schedule 1
Subject Matter and Details of Processing

Customer / 'Data Exporter' Details

Name:	Customer
Contact details for data protection:	Qualtrics will contact the contact person named in the applicable EULA Acceptance Form
Main address:	Customer address listed in the applicable EULA Acceptance Form
Customer activities:	Purchasing a license for Cloud Services as described in the applicable EULA Acceptance Form
Role:	Controller

Provider / 'Data Importer' Details

Name:	Qualtrics
Contact details for data protection:	Data Protection Officer, privacy@qualtrics.com
Main address:	333 W River Park Drive, Provo, Utah 84604, USA
Provider activities:	Delivery of Cloud Services and associated services (if applicable) as described in the applicable EULA Acceptance Form
Role:	Processor

Details of Processing

Categories of Data Subjects:	Determined by Customer or Permitted Controllers. Unless otherwise indicated by Customer or Permitted Controller, transferred Personal Data relates to the Data Subjects having Personal Data (a) stored in the Cloud Service or (b) transmitted to, made available to, accessed by, or otherwise processed by the data importer.
Categories of Personal Data:	Determined by Customer or Permitted Controllers. Customer or Permitted Controllers may 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, email address, address data, system access / usage / authorization data, company name, contract data, invoice data, and any application-specific data that Authorized Users transfer or enter into the Cloud Service.
Special Categories of Personal Data and additional associated restrictions/safeguards:	Determined by Customer or Permitted Controllers. If Customer or a Permitted Controller intends to collect Special Categories of Personal Data, it will be specified in the applicable EULA Acceptance Form. For purposes hereof, "Special Categories of Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

	Qualtrics has taken Technical and Organizational Measures to ensure a level of security appropriate to protect Special Categories of Personal Data. The transfer of Special Categories of Personal Data may trigger the application of the following additional restrictions or safeguards if necessary, taking 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): 1. training of personnel; 2. encryption of data in transit and at rest; and 3. system access logging and general data access logging. In addition, the Cloud Service may provide measures for handling Special Categories of Personal Data as described in the Documentation.
Frequency of transfer:	Personal Data will be transferred on an ongoing basis for the duration of the Agreement.
Nature of the Processing:	The transferred Personal Data is subject to the following basic processing activities: 1. use of Personal Data to set up, operate, monitor, and provide the Cloud Service (including operational and technical support); 2. provision of professional services; 3. communication to Authorized Users; 4. storage of Personal Data in dedicated data centers (multi-tenant architecture); 5. release, development, and upload of any fixes or upgrades to the Cloud Service; 6. back up and restoration of Personal Data stored in the Cloud Service; 7. computer processing of Personal Data, including data transmission, data retrieval, and data access; 8. network access to allow Personal Data transfer; 9. monitoring, troubleshooting, and administering the underlying Cloud Service infrastructure and database; 10. security monitoring, network-based intrusion detection support, and penetration testing; and 11. execution of instructions of Customer in accordance with the Agreement.
Purpose of the Processing:	The purpose of the transfer is to provide and support the Cloud Service and any associated services. Qualtrics and its Subprocessors may support the Cloud Service data centers remotely.
Duration of Processing / retention period:	Personal Data will be retained for the duration of the Agreement and subject to Section 5 of the DPA.
Transfers to Subprocessors:	Transfers to Subprocessors will be on the same basis as set out in the DPA.

Schedule 2
Technical and Organizational Measures

This Schedule 2 describes 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 involves Restricted Transfers, the Technical and Organizational Measures set forth in Schedule 2 describe the measures and safeguards that have been taken to fully take into consideration the nature of the personal data and the risks involved.

1. TECHNICAL AND ORGANIZATIONAL MEASURES

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings, or rooms where data processing systems that process 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, 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, security guards, 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 at reception and must be accompanied by authorized Qualtrics personnel.
- Physical logs are maintained, along with logs for all access events through the access control system.
- 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.
- Physical access logs are maintained, along with logs for all access events through the access control system.

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 through defined processes according to 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 Qualtrics' security policy (for example, no rights are granted without authorization). In case personnel leave the company, their access rights are revoked in a timely manner.
- Employment at Qualtrics is contingent on completion of background checks, as permitted by applicable law.
- Qualtrics has established a password policy that defines complexity requirements and 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. All personnel are assigned personalized user IDs for authentication. All passwords are stored in encrypted form. Each computer has a password-protected screensaver and defined time-out period due to inactivity.
- Full remote access to Qualtrics' corporate network and critical infrastructure is protected by strong authentication.
- Disciplinary procedures are defined for non-adherence to Qualtrics' policies by employees.

1.3 **Data Access Control.** Persons entitled to use data processing systems gain access only to 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, considering the privilege of least principle, and requires the use of multifactor authentication (MFA) on the account and connection to the Qualtrics network either locally or virtually (VPN). Personnel have access to the information that they require to fulfill their duty. Qualtrics uses authorization concepts that grant assigned roles per account (user ID). All Customer Data is protected in accordance with the Qualtrics suite of information security policies.
- All production servers are operated in the data centers. 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 the Cloud Service.
- A 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.

Measures:

- Personal Data in transfer over Qualtrics internal networks is protected via industry-recognized encryption practices according to Qualtrics' security policy.
- When data is transferred between Qualtrics and its customers, the protection measures for the transferred Personal Data make use of industry-recognized encryption practices. 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).
- Qualtrics offers functionality within the Cloud Service for Customer to target its anonymization and pseudonymization preferences.

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:

- Various tools are used to monitor the confidentiality, integrity, availability, and performance of the Cloud Service, across Qualtrics' networks and hosts, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), performance and health systems, and security event correlation systems.
- 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.
- System and performance logs are sent to a security information and event management (SEIM) system for long-term storage.
- The SEIM system is configured to monitor and alert when certain thresholds and activities are performed.
- Alert notifications are monitored by Qualtrics' security operations center (SOC).

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 maintains software development lifecycle and change management procedures aligned to recognized industry practice.
- The change management process requires that all changes be documented, risk-assessed, prioritized, planned, tested, approved, and implemented.
- Source code is processed via static application security testing (SAST) and dynamic application security testing (DAST) tooling.
- Separate development, testing, and production environments are established.
- Segregation of duties (SoD) is achieved as code is reviewed and approved by different individuals prior to applicable deployments.
- Qualtrics establishes agreements with third parties and Subprocessors that subject third parties and Subprocessors to equivalent confidentiality, security posture, and controls as those that Qualtrics maintains itself, per the nature of the services rendered, in line with Qualtrics' security policy.
- Qualtrics employees are held to similar expectations with established employee agreements and confidentiality commitments and adhere to Qualtrics' company policies.
- At least annual information security, privacy, and compliance training is conducted for relevant employees.

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 (e.g., UPS, batteries, generators, etc.) to protect power availability to the data centers.
- Qualtrics has defined business continuity and disaster recovery plans for business-critical processes.

- Emergency processes, disaster recovery, and backup restoration capabilities are regularly tested.
- Data center providers use geographically resilient locations.

1.8 **Data Separation Control.** Personal Data between tenants will be separated in line with recognized industry practice to ensure confidentiality, availability, and appropriate applicability between customers.

Measures:

- Qualtrics uses the technical capabilities of the deployed software (e.g., multi- tenancy, system landscapes) to achieve logical data separation between Personal Data originating from multiple customers.
- Customer (including Permitted 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:

- Separate corporate, development, and production environments are maintained.
- The company network is protected from the public network by firewalls.
- Qualtrics uses up-to-date antivirus/anti-malware software at access points to the company network (for email accounts), as well as on all file servers and all workstations.
- External and internal penetration efforts are conducted at least annually.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates.
- Qualtrics has established incident response procedures aligned with recognized industry practice, including data breach notification commitments.
- Incident response plans are regularly tested.

Schedule 3
Restricted Transfers

1. Definitions.

1.1 "**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. For the avoidance of doubt, if the EU Standard Contractual Clauses apply, then Modules 2 and 3 will apply as set forth in Schedule 3.

1.2 "**FADP**" means the Swiss Federal Act on Data Protection.

1.3 "**GDPR**" means the General Data Protection Regulation 2016/679.

1.4 "**Restricted Transfer**" means a transfer (or an onward transfer) of Personal Data to a Third Country (as defined below) if (a) such transfer requires an adequacy means pursuant to GDPR or other Data Protection Law and (b) such adequacy means may be met by the parties entering into the EU Standard Contractual Clauses.

1.5 "**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.

1.6 "**UK GDPR**" means the GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. Transfers.

2.1 **EU Transfers**. If Personal Data is protected by GDPR and is subject to a Restricted Transfer, the following applies:

(a) The EU Standard Contractual Clauses are hereby incorporated by reference as follows:

(1) If Qualtrics is located in a Third Country:

(A) Customer is the "data exporter" and Qualtrics is the "data importer";

(B) Module 2 (Controller to Processor) applies if Customer is a controller of Personal Data and Qualtrics is a processor of Personal Data;

(C) Module 3 (Processor to Processor) applies if Customer is a processor of Personal Data (on behalf of a third-party controller) and Qualtrics is a processor of Personal Data; and

(D) each party is deemed to have signed the EU Standard Contractual Clauses (including their Annexes) as of the effective date of the DPA, and Customer enters into the EU Standard Contractual Clauses on behalf of itself and Permitted Controllers (if any).

(2) For any Restricted Transfer from Qualtrics to its Subprocessors, Qualtrics and its Subprocessors have entered into the EU Standard Contractual Clauses.

(b) For each Module (if applicable):

(1) the optional docking clause in Clause 7 does not apply;

(2) in Clause 9, Option 2 will apply; the minimum time period for prior notice of Subprocessor changes will be as set out in the DPA; and Qualtrics will fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with the DPA;

(3) in Clause 11, the optional language does not apply;

(4) in Clause 13(a), the second two paragraphs do not apply;

(5) in Clause 17, Option 1 will apply, and the EU Standard Contractual Clauses will be governed by the laws of Ireland;

(6) in Clause 18(b), disputes will be resolved before the courts of Ireland;

(7) Schedule 1 (Subject Matter and Details of Processing) to the DPA contains the information required in Annex 1 of the EU Standard Contractual Clauses; and

(8) Schedule 2 (Technical and Organizational Measures) to the DPA contains the information required in Annex 2 of the EU Standard Contractual Clauses.

(c) If context permits and requires, any reference in the DPA to the EU Standard Contractual Clauses will be read as a reference to the EU Standard Contractual Clauses as modified in the manner set forth in this section.

(d) If 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 applicable data exporter will have the following third-party beneficiary right: If 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 Customer by contract or by operation of law), the applicable data exporter may terminate the affected Cloud Service solely to the extent that the data exporter's Personal Data is processed, in which case the applicable data exporter also instructs Qualtrics to erase or return the Personal Data in accordance with the DPA.

(e) Nothing in the Agreement will be construed to prevail over any conflicting clause of the EU Standard Contractual Clauses. For the avoidance of doubt, the audit and subprocessor rules in the DPA also apply in relation to the EU Standard Contractual Clauses.

2.2 **Swiss Transfers**. If Personal Data is protected by the FADP and is subject to a Restricted Transfer, the EU Standard Contractual Clauses apply as set forth in Section 2.1 (EU Transfers) of this Schedule 3 with the following modifications:

(a) in Clause 13, the competent supervisory authority will be the Swiss Federal Data Protection and Information Commissioner, or if both the FADP and the GDPR apply to such transfer, one of the competent data protection authorities under the EU Standard Contractual Clauses;

(b) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland;

(c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;

(d) the terms used in the EU Standard Contractual Clauses that are defined in the FADP will be construed to have the meaning set forth in the FADP;

(e) the term Member State will not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c);

(f) if the FADP protects legal entities as data subjects, the EU Standard Contractual Clauses will apply to data relating to identified or identifiable legal entities;

(g) references to the law of the European Union or of a Member State in the EU Standard Contractual Clauses will be deemed to be a reference to the FADP; and

(h) references to a Member State in the EU Standard Contractual Clauses will be deemed to include Switzerland.

2.3 **UK Transfers.** If Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the EU Standard Contractual Clauses apply as set forth in Section 2.1 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party will be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU Standard Contractual Clauses will be deemed amended as specified by the UK Addendum in respect of the transfer of Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to the DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU Standard Contractual Clauses, modules, and selected clauses that this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(1) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to the DPA;

(2) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to the DPA;

(3) Annex II is located in Schedule 2 (Technical and Organizational Measures) to the DPA and

(4) the list of Subprocessors is located in the DPA.

(f) in Table 4 of the UK Addendum, the Importer may end the UK Addendum in accordance with its terms (and the applicable box is deemed checked); and

(g) in Part 2: 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 section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses, will be deemed to apply.