




Order Form

Parties:	Qualtrics, LLC 333 W. River Park Dr. Provo, UT 84604 United States ("Qualtrics")	Temecula Valley Unified School District School Facilities 31350 Rancho Vista Rd Temecula, CA 92592 United States ("Customer")
Effective Date:	The date signed by the last party to sign.	
Governing Document:	This Order Form is subject to the General Terms and Conditions between the parties dated on or about the date hereof (the " Agreement "). All capitalized terms used but not defined herein have the meanings given to them in the Agreement. If there is a conflict between the terms of the Agreement and this Order Form, this Order Form will control.	
Attachments:	<ul style="list-style-type: none"> - Service Level Exhibit - Fees Exhibit - Cloud Service Exhibit - Professional Services Exhibit 	
Services:	As set forth in the exhibits attached hereto	
Term:	As set forth in the exhibits attached hereto	
Payment Terms:	As set forth in the exhibits attached hereto	
Additional Terms:		
To be completed by Customer		
Regional Data Center:	US	Purchase Order Number (if any):
Email Address for Invoice Submission:	dliane@tvusd.k12.ca.us	Shipping Address:
Invoicing Instructions (if applicable):	Billing Address for Invoice Submission:	31350 Rancho Vista Rd Attn: Temecula Valley Unified School District School Temecula Valley USD Temecula CA United States 92592

Qualtrics	Customer
By (signature): 	By (signature):
Name: Mark Creer	Name:
Title: Director	Title:
Date: February 02, 2021	Date:
Qualtrics Primary Contact:	Customer Primary Contact:
Name: Mahonri Pacanos	Name: Donna Lione
Phone: (385) 203-4506	Phone: (951) 428-7488
Email: mahonrip@qualtrics.com	Email: dliane@tvusd.k12.ca.us



Order Form

Service Level Exhibit

Service Levels

1. **Availability.** Qualtrics will use commercially reasonable efforts to ensure that the Cloud Service will be available at all times, excluding when the Cloud Service is unavailable due to (a) required system maintenance as determined by Qualtrics ("**Scheduled Maintenance**"); and (b) causes outside of the reasonable control of Qualtrics that could not have been avoided by its exercise of due care, including any outages caused by: (i) the Internet in general; (ii) a Customer-caused event; or (iii) any Force Majeure Event ("**Availability**").
2. **Scheduled Maintenance.** A minimum of five days' advance notice will be provided by email to Customer for all Scheduled Maintenance exceeding two hours. For Scheduled Maintenance lasting less than two hours, notice will be displayed on the login page.
3. **Downtime.** "**Downtime**" is defined as the Cloud Service having no Availability, expressed in minutes.
4. **Remedies for Downtime.** If Downtime exceeds a certain amount per month, Customer will be entitled, upon written request, to a credit ("**Fee Credit**") based on the formula: Fee Credit = Fee Credit Percentage set forth below * (1/12 current annual Fees paid for Software affected by Downtime). All times listed immediately below are per calendar month.
 1. If Downtime is 30 minutes or less, no Fee Credit Percentage is awarded.
 2. If Downtime is from 31 to 120 minutes, Customer is eligible for a Fee Credit Percentage of 5%.
 3. If Downtime is from 121 to 240 minutes, Customer is eligible for a Fee Credit Percentage of 7.5%.
 4. If Downtime is 241 minutes or greater, Customer is eligible for a Fee Credit Percentage of 10.0%



Order Form

Fees Exhibit

License Details

Start Date	End Date	Term in Months
25-Jan-2021	24-Jan-2022	12

Cloud Service Details

Year	Services	Price	Estimated Invoice Date	Payment Terms from Invoice	License Configuration
1	Cloud Professional	\$58,000.00 \$1,500.00	Effective Date	Net 30	Q-1389972
Total		USD \$59,500.00			

Prices shown do not include applicable taxes. Applicable taxes will be presented on the invoice.

Press Release

Notwithstanding anything to the contrary in the Agreement, upon mutual execution of this Order Form Customer grants Qualtrics the right to issue a press release naming Customer as a customer of Qualtrics and identifying the product purchased.



Order Form

Cloud Service Exhibit

Cloud Service Renewal (not applicable to pilots or proofs of concept). Qualtrics sends renewal notices to customers at least 60 days before the end of the term. Upon expiration of each term, the Cloud Service may be renewed for a successive one-year term with a price increase of no more than 5% at such renewal upon written agreement.

[Description of Services on following page]



Order Form

YEAR 1
Q-1389972

CLOUD SERVICE

EmployeeXM for Internal Support

Website Feedback
Developer Tools
EmployeeXM for Internal Support Core : 1000
SMS Text Reserve : up to 150000
Dashboards
Directory
Expert Content : 3
In-App Feedback
Included Projects : 3
Actions
Communication & Chat Integration
Customer Support/Help Desk Integrations
SMS Integration
Surveys & Distribution
Text IQ
Ticketing/Closed-Loop
SSO



Order Form

Professional Services Exhibit: SSO Configuration

Customer agrees that Qualtrics may use subcontractors to deliver any portion(s) of the Project at Qualtrics' discretion.

1. Definitions

- a. "Delivery Team" refers to the SET of resources assigned for fulfillment of project scope. "Project" refers to the SSO Configuration to be provided under this Professional Services Exhibit.
- b. "Standard Business Hours" are 0900 to 1700 hours according to the time zone of the office in which Delivery Team is located, unless otherwise agreed to in writing during the Project.

2. Project Scope

- a. Inclusions
 - i. SSO (Single Sign-On) Configuration
- b. Assumptions
 - i. For the duration of the Project, Customer will provide the Delivery Team with access to Customer's Qualtrics brand (account) as a brand administrator.

3. Responsibilities

- a. Delivery Team Responsibilities
 - i. Provide documentation, specifications, and requirements for SSO set-up.
 - ii. Conduct Q&A session with Customer and Customer IT/SSO team to identify any potential roadblocks, including a non-standard SSO system.
 - iii. Configure a test brand to validate SSO setup.
 - iv. Provide configuration details for the test brand and a login URL for setup validation.
 - v. Provide support in troubleshooting any errors that arise in the test instance.
 - vi. Test the SSO setup within a test brand before transferring to the live brand.
 - vii. After successful testing of the configuration, provide configuration details to the Customer for the live brand, then transfer the configuration to the live brand.
- b. Customer Responsibilities
 - i. Provide key configuration details of SSO system as requested by Qualtrics, dependent on the type of SSO connection.
 - ii. If customer SSO can support it, ensure SSO is set up to pass any user attributes required for dashboard permissioning.
 - iii. Ensure that a user in the Customer's IdP can successfully login to the Qualtrics platform using their SSO credentials.
 - iv. Manages User Acceptance Testing ("UAT") process and any special testing requirements.

4. Governance

- a. Delivery Team will reach out to Customer after completion of request survey within the timeline specified in request survey to schedule a Project kickoff call or coordinate via email. Timing of kickoff call will be mutually agreed between Delivery Team and Customer based on Delivery Team availability and Customer's milestones.
- b. The Project is complete based on completion of delivery and Customer's acceptance, per the terms of the Acceptance Criteria section.
- c. Unless otherwise agreed by both parties in writing, all interactions and meetings will be conducted in English, and will be conducted remotely, via phone, email, or videoconference.

5. Acceptance Criteria

- a. Once SSO Configuration is completed and the Delivery Team provides notification for review and approval, the Customer will either (1) confirm the requirements have reasonably been met and sign off on the approval or (2) reply to the Delivery Team, in writing, detailing the specific requirements that must still be met. Upon mutual agreement, both parties may agree to extend the time period for UAT, though additional time may impact Project timelines and budget and be subject to a Change Order (as defined below).
- b. SSO Configuration will be reviewed and signed off according to the following process:
 - i. Delivery Team will provide configuration details to the Customer for the live brand and transfer the configuration to the live brand at least 5 business days prior to the Deliverable completion date.
 - ii. Customer will sign off or report any issues within 5 business days of submission.
 - iii. The Delivery Team will correct reported issues within a mutually agreed time frame.
 - iv. Customer will provide written feedback and raise issues related to the reworked portion within a mutually agreed time frame, and the Delivery Team will make changes necessary to resolve the issues.
 - v. Customer will provide final review and signoff within 2 business days.
 - vi. SSO Configuration will be considered accepted if the Customer does not provide written notification of SSO Configuration rejection within the timelines specified above.

6. Third Party Vendors and Products

- a. Customer remains responsible for their own vendors and third parties providing services related hereto.
- b. Qualtrics is not responsible for third party products obtained by Customer.

7. Change Orders

- a. If Customer or Delivery Team wishes to change the scope of the Project, they will submit details of the requested change to the other in writing. Delivery Team will, within a reasonable time after such request is received, provide a written estimate to Customer of changes to Project cost, timeline, and/or scope.
- b. Promptly after receipt of the written estimate, Customer and Delivery Team will negotiate and agree in writing on the terms of such change (a "Change Order"). Each Change Order complying with this Section will be considered an amendment to this Service Order.

8. Payments and Fees

Item	Invoice Date	Price (USD)
Standard SSO Configuration		\$1,500.00
Total:		\$1,500.00

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 Order Form.

3.3 Security.

Qualtrics will implement and maintain appropriate 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")** for Cloud Services incorporated into the Order Form in compliance with applicable data protection law.

3.4 Modifications.

- (a) The Cloud Service and Qualtrics Policies may be modified by Qualtrics. Qualtrics will inform Customer of modifications by email, the support portal, release notes, Documentation or the Cloud Service. The information will be delivered by email if the modification is not solely an enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.
- (b) If Customer establishes that a modification is not solely an enhancement and materially reduces the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to Qualtrics within thirty days after receipt of Qualtrics' informational notice.

3.5 Analyses.

Qualtrics or Qualtrics' Affiliates may create analyses utilizing, in part, Customer Data and information derived from Customer's use of the Cloud Service and Consulting Services, as set forth below ("**Analyses**"). Analyses will anonymize, deidentify and aggregate information and will be treated as Cloud Materials.

Unless otherwise agreed, personal data contained in Customer Data is only used to provide the Cloud Service and Consulting Services. Analyses may be used for the following purposes:

- a) product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new Qualtrics products and services,
- b) improving resource allocation and support,
- c) internal demand planning,
- d) training and developing machine learning algorithms,
- e) improving product performance,
- f) verification of security and data integrity
- g) identification of industry trends and developments, creation of indices and anonymous benchmarking

4. CUSTOMER AND PERSONAL DATA

4.1 Customer Data.

Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to Qualtrics (including Qualtrics' Affiliates and subcontractors) a nonexclusive right to process Customer Data solely to provide and support the Cloud Service. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are in accordance with Education Code section 49073.1.

4.2 Personal Data.

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

4.3 Security.

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct or authorize penetration tests of the Cloud Service without advance approval from Qualtrics.

4.4 Processing of Customer Data.

All Customer data shall be processed in the data center region selected by Customer except to the extent necessary to comply with Customer's instructions (e.g. support purposes, use of subprocessor services) or as strictly necessary to provide the Cloud Service.

4.5 Access to Customer Data.

- (a) During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer 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 Customer Data.
- (b) Before the Subscription Term expires, if available, Customer may use Qualtrics' self-service

export tools (as available) to perform a final export of Customer Data from the Cloud Service. Alternatively, Customer may request data export through support ticket.

- (c) At the end of the Agreement, Qualtrics will delete the 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.
- (d) In the event of third party legal proceedings relating to the Customer Data, Qualtrics will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

5. FEES AND TAXES

5.1 Fees and Payment.

Customer will pay fees as stated in the Order Form. After prior written notice, Qualtrics may suspend Customer's use of the Cloud Service until payment is made. Customer cannot withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable and fees non-refundable.

5.2 Taxes.

Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than Qualtrics' income and payroll taxes. Customer must provide to Qualtrics any direct pay permits or valid tax-exempt certificates prior to signing an Order Form. If Qualtrics is required to pay taxes (other than its income and payroll taxes), Customer will reimburse Qualtrics for those amounts and indemnify Qualtrics for any taxes and related costs paid or payable by Qualtrics attributable to those taxes.

6. TERM AND TERMINATION

6.1 Term.

The Subscription Term is as stated in the Order Form.

6.2 Termination.

A party may terminate the Agreement:

- (a) upon thirty days written notice of the other party's material breach unless the breach is cured during that thirty day period,
- (b) as permitted under Sections 3.4(b), 7.3(b), 7.4(c), or 8.1(c) (with termination effective thirty days after receipt of notice in each of these cases), or
- (c) immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

6.3 Refund and Payments.

For termination by Customer or an 8.1(c) termination, 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 date of termination, and
- (b) a release from the obligation to pay fees due for periods after the effective date of termination.

6.4 Effect of Expiration or Termination.

Upon the effective date of expiration or termination of the Agreement:

- (a) Customer's right to use the Cloud Service and all Qualtrics Confidential Information will end,
- (b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and
- (c) termination or expiration of the Agreement does not affect other agreements between the parties.

6.5 Survival.

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

7. WARRANTIES

7.1 Compliance with Law.

Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:

- (a) in the case of Qualtrics, the operation of Qualtrics' business as it relates to the Cloud Service, and
- (b) in the case of Customer, the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices.

Qualtrics warrants that it 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 Remedy.

If Qualtrics corrects the warranted non-conformity, that correction shall be full satisfaction of Qualtrics' obligation (and Customer shall waive all claims) in connection to a breach of the limited warranty in Sections 7.1 and 7.2. If Qualtrics fails to correct the warranted non-conformity after using reasonable commercial efforts, Qualtrics may terminate access to the non-conforming Cloud Service and (a) offer to refund the subscription fees paid by Customer for such non-conforming Cloud Service (as identified in the applicable Order Form) for the remainder of the subscription term (starting on the date Customer reported the non-conformity) in full and final settlement of all claims in connection to a breach of the limited warranty in Sections 7.1 and 7.2, or (b) if Customer rejects the offer of such refund, Customer may choose to exercise any rights available to it under the Agreement and applicable law, subject to payment for the period of the Cloud Service made available to Customer prior to Customer reporting the non-conformity.

~~(a) —~~

7.4 Warranty Exclusions.

The warranties in Sections 7.2 and 7.4 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 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 provided in the Agreement, neither Qualtrics nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of Qualtrics or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1 Claims Brought Against Customer.

- (a) Qualtrics will defend Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's and 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 finally awarded against Customer (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 (i) Customer's breach of Section 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by Qualtrics, or (iii) use of the Cloud Service provided for no fee.
- (c) In the event a claim is made or likely to be made, Qualtrics may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, Qualtrics or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

8.2 Claims Brought Against Qualtrics.

Customer will defend 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 finally awarded against Qualtrics and its Affiliates and subcontractors (or the amount of any settlement Customer enters into) with respect to these claims.

Customer shall have no obligation to indemnify, defend, or hold harmless Qualtrics for Qualtrics' sole negligence or willful misconduct.

8.3 Third Party Claim Procedure.

- (a) The party against whom a third party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.
- (b) The party that is obligated to defend a claim will have the right to fully control the defense.
- (c) Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought.

8.4 Exclusive Remedy.

The provisions of Section 8 state the sole, exclusive, and entire liability of the parties, their Affiliates, Business Partners 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 will exclude or limit its liability for damages resulting from:

- (a) the parties' obligations under Section 8.1(a) and 8.2,
- (b) unauthorized use or disclosure of Confidential Information,
- (c) either party's breach of its data protection and security obligations that result in an unauthorized use or disclosure of personal data,
- (d) death or bodily injury arising from either party's gross negligence or willful misconduct, or
- (e) any failure by Customer to pay any fees due under the Agreement.

9.2 Liability Cap.

Subject to Sections 9.1 and 9.3, the maximum aggregate liability of either party (or its respective Affiliates or Qualtrics' subcontractors) or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period. Any "twelve 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:

- (a) neither party (nor its respective Affiliates or Qualtrics' subcontractors) will be liable to the other party for any special, incidental, consequential, or indirect damages, loss of good will or business profits, work stoppage or for exemplary or punitive damages, and
- (b) Qualtrics will not be liable for any damages caused by any Cloud Service provided for nofee.

9.4 Risk Allocation.

The Agreement allocates the risks between Qualtrics and Customer. The fees for the Cloud Service and Consulting Services reflect this allocation of risk and limitations of liability.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 QUALTRICS Ownership.

Qualtrics, Qualtrics' Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to Qualtrics and its licensors.

10.2 Customer Ownership.

Customer retains all rights in and related to the Customer Data. Qualtrics may use Customer-provided trademarks solely to provide and support the Cloud Service.

10.3 Non-Assertion of Rights.

Customer covenants, on behalf of itself and its successors and assigns, not to assert against Qualtrics and its Affiliates or licensors, any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Consulting Services.

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

- (a) The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users 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 substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.
- (b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.
- (c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.

11.2 Protection of Confidential Student Data and FERPA.

Qualtrics will comply with the Family Educational Rights and Privacy Act of 1974 ("FERPA") as a "school official") to the extent that such law imposes obligations directly upon Qualtrics as a Processor in connection with the Cloud Service specified in the Order Form and Customer shall comply with FERPA to the extent that such law imposes obligations directly upon Customer as a Controller in connection with the Cloud Service specified in the Order Form. Additionally, in accordance with California Education Code section 49073.1, Customer and Qualtrics agree to the following terms and procedures to protect the privacy of confidential student records:

- (a) "Student records" include any information directly related to a student that is maintained by Customer or acquired directly from the student through the use of instructional software or applications assigned to the pupil by a teacher or other Customer employee. "Student records" does not include deidentified information, including aggregated deidentified information, used by Qualtrics: (1) to improve educational products, for adaptive learning purposes, and for customizing student learning; (2) to demonstrate the effectiveness of Qualtrics' products in the marketing of those products; or (3) for the development and improvement of educational sites, services, or applications.
- (b) As between Qualtrics and Customer, Student records obtained by Qualtrics from Customer continue to be the property of and under the control of Customer.
- (c) The procedures by which students may retain possession and control of their own student-generated content are outlined as follows: (1) Customer shall maintain full control of student-generated data and shall have unrestricted access; (2) upon a request, Customer shall provide students and parents with access to student-generated content; and (3) Qualtrics shall not provide student records to parents or students.
- (d) The options by which a student may transfer student-generated content to a personal account include: (1) submitting a written request to Customer; and (2) Qualtrics shall not provide student-generated content to students directly.
- (e) Parents, legal guardians, or eligible students may review personally identifiable information in the student's records and correct erroneous information by the following protocol: (1) submitting a written request to Customer; and (2) any changes to student records shall be made by Customer.
- (f) Qualtrics and Customer shall take actions to ensure the security and confidentiality of student records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of student records, by the following measures: (1) limiting access to the services to only those who possess an individualized username and password; (2) use of encryption when storing information on the Qualtrics' servers; and (3) compliance with the terms and conditions of this Agreement.
- (g) In the event of an unauthorized disclosure of a student's records, Customer shall report to an affected parent, legal guardian, or eligible student pursuant to the following procedure: (1) Qualtrics shall notify Customer of any confirmed unauthorized disclosure and such notification shall include a description of the nature and extent of the disclosure; and (2) Customer shall notify the affected parent, legal guardian, or eligible student.
- (h) Qualtrics shall not use any information in a student record for any purpose other than those required or specifically permitted by the Agreement. Qualtrics shall not use personally identifiable information in student records to engage in targeted advertising.
- (i) Qualtrics certifies that a student's records shall not be retained or available to Qualtrics upon completion of the terms of the Agreement. Such certification will be enforced through compliance with the terms and condition of this Agreement.
- (j) Customer and Qualtrics will agree to work with Qualtrics to ensure compliance with FERPA by complying with the terms and conditions of this Agreement.

11.3 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) is generally available to the public without breach of the Agreement by the receiving party,
- (c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or
- (d) the disclosing party agrees in writing is free of confidentiality restrictions.

11.4 Publicity.

Neither party will use the name of the other party in publicity activities without the prior written consent of the other, except that Customer agrees that Qualtrics may use Customer's name in customer listings or quarterly calls with its investors or, at times mutually agreeable to the parties, as part of Qualtrics' marketing efforts (including reference calls and stories, press testimonials, site visits, SAPPHIRE participation). Customer agrees that Qualtrics may share information on Customer with its Affiliates for internal business purposes and that it has secured appropriate authorizations to share Customer employee contact information with Qualtrics.

12. MISCELLANEOUS

12.1 Severability.

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

12.2 No Waiver.

A waiver of any breach of the Agreement is not deemed a waiver of any other breach.

12.3 Electronic Signature.

Electronic signatures that comply with applicable law are deemed original signatures.

12.4 Regulatory Matters.

Qualtrics Confidential Information is subject to export control laws of various countries, including the laws of the United States and Germany. Customer will not submit Qualtrics Confidential Information to any government agency for licensing consideration or other regulatory approval, and will not export Qualtrics Confidential Information to countries, persons or entities if prohibited by export laws. With regards to export control laws, in the event of a conflict between United States and/or California law and any other country's export control laws, the United States and/or California export control laws shall control.

12.5 Notices.

All notices will be in writing and given when delivered to the address set forth in an Order Form with copy to the legal department. Notices by Qualtrics relating to the operation or support of the Cloud Service and those under Sections 3.4 and 5.1 may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Order Form.

12.6 Assignment.

Without Qualtrics' prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. Qualtrics may assign the Agreement to Qualtrics Affiliates. In the event Qualtrics assigns the Agreement to one or more of its Affiliates, the Affiliates shall comply with, and be subject to all terms and conditions described in this Agreement.

12.7 Subcontracting.

Qualtrics may subcontract parts of the Cloud Service or Consulting Services to third parties. Qualtrics is responsible for breaches of the Agreement caused by its subcontractors.

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. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 Governing Law.

The Agreement and any claims relating to 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. All disputes will be subject to the exclusive jurisdiction of the courts located in New Castle County, Delaware. 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. Either party must initiate a cause of action for any claim(s) relating to the Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

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. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the Agreement and the parties disclaim any reliance on them. The Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if Qualtrics accepts or does not otherwise reject the purchase order.

12.12 Data Processing Agreement.

Where Customer is processing personal data using the Services, the DPA shall govern the processing of such personal data.

Glossary

- 1.1 "Affiliate"** of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.
- 1.2 "Agreement"** means an Order Form and documents incorporated into an Order Form.
- 1.3 "Authorized User"** means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor or representative of
- (a) Customer,
 - (b) Customer's Affiliates, and/or
 - (c) Customer's and Customer's Affiliates' Business Partners.
- 1.4 "Business Partner"** means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.
- 1.5 "Cloud Service"** means any distinct, subscription-based, hosted, supported and operated on- demand solution provided by Qualtrics under an Order Form.
- 1.6 "Cloud Materials"** mean any materials provided or developed by Qualtrics (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.
- 1.7 "Confidential Information"** means
- (a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and
 - (b) with respect to Qualtrics: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding Qualtrics research and development, product offerings, pricing and availability.
 - (c) Confidential Information of either Qualtrics or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.
- 1.8 "Consulting Services"** means professional services, such as implementation, configuration, custom development and training, performed by Qualtrics' employees or subcontractors as described in any Order Form and which are governed by the Supplement for Consulting Services or similar agreement.
- 1.9 "Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a 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 will not include Qualtrics' Confidential Information.
- 1.10 "Documentation"** means Qualtrics' then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.
- 1.11 "Order Form"** means the ordering document for a Cloud Service that references the GTC.
- 1.12 "Qualtrics Policies"** means the operational guidelines and policies applied by Qualtrics to provide and support the Cloud Service as incorporated in an Order Form.
- 1.13 "Subscription Term"** means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.
- 1.14 "Supplement"** means as applicable, the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.
- 1.15 "Usage Metric"** means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.

THE PARTIES ENTER INTO THIS AGREEMENT AS OF THE LAST SIGNATURE DATE BELOW ("GTC EFFECTIVE DATE").


CUSTOMER:	QUALTRICS, LLC
By:	By: 
Name:	Name: Mark Creer
Title:	Title: Director
Date:	Date: February 02, 2021

Exhibit A
Data Processing Agreement

PERSONAL DATA PROCESSING AGREEMENT FOR QUALTRICS CLOUD SERVICES

This Data Processing Addendum ("DPA") is entered into

BETWEEN

(1) Customer; and

(2) Qualtrics.

1. BACKGROUND

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

1.2 Structure. Appendices 1 and 2 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 and the applicable technical and organizational measures.

1.3 GDPR. Qualtrics and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 Governance. Qualtrics acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining 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 and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

2. SECURITY OF PROCESSING

2.1 Appropriate Technical and Organizational Measures. Qualtrics has implemented and will apply the technical and organizational measures set forth in [Appendix 2](#). 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.

2.2 Changes. Qualtrics applies the technical and organizational measures set forth in Appendix 2 to Qualtrics' entire customer base hosted out of the same Data Center and receiving the same Cloud Service. Qualtrics may change the measures set out in Appendix 2 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 PersonalData.

3. QUALTRICS OBLIGATIONS

3.1 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).

- 3.2 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.
- 3.3 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.
- 3.4 Cooperation.** 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. Qualtrics shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. Qualtrics shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, Qualtrics will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.
- 3.5 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.
- 3.6 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 or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

- 4.1 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.
- 4.2 Deletion.** Before the Subscription Term expires, Customer is required to 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 six months) unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

- 5.1 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 and/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) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

- 5.2 Other Controller Audit.** Any other Controller may audit Qualtrics' control environment and security practices relevant to Personal Data processed by Qualtrics in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 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.
- 5.3 Scope of Audit.** Customer shall provide at least sixty 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 three 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.
- 5.4 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.

6. SUBPROCESSORS

- 6.1 Permitted Use.** Qualtrics is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:
- (a) Qualtrics 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 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.
- 6.2 New Subprocessors.** Qualtrics' use of Subprocessors is at its discretion, provided that:
- (a) Qualtrics will inform Customer in advance (by email or by posting within 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 6.3.
- 6.3 Objections to New Subprocessors.**
- (a) 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 thirty days from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.
 - (b) Within the thirty day period from the date of Qualtrics' notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss 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 thirty day period.
 - (c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.
- 6.4 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 6.3 applies accordingly.
- ## **7. INTERNATIONAL PROCESSING**
- 7.1 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.

- 7.2 Standard Contractual Clauses.** Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as a safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:
- (a) Qualtrics and Customer enter into the Standard Contractual Clauses;
 - (b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by Qualtrics and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by Qualtrics) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when Qualtrics has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or
 - (c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with Qualtrics and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.
- 7.3 Relation of the Standard Contractual Clauses to the Agreement.** Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.
- 7.4 Governing Law of the Standard Contractual Clauses.** The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. 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.

9. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

- 9.1 "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.
- 9.2 "Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in the region agreed in an Order Form.
- 9.3 "Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by Qualtrics on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).
- 9.4 "Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.
- 9.5 "EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
- 9.6 "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 (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) 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).

- 9.7** **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) 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.
- 9.8** **"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.
- 9.9** **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.
- 9.10** **"Subprocessor"** means Qualtrics affiliates and third parties engaged by Qualtrics in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

Qualtrics and its Subprocessors provide the Cloud Service that includes the following support:

Qualtrics and its Affiliates support the Cloud Service data centers remotely from Qualtrics' locations specified in Qualtrics' Security White Paper (which is available upon request). Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

Qualtrics and its Affiliates provide support when a Customer requests support because the Cloud Service is not available or not working as expected for some or all Authorized Users. Qualtrics answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

The Data Exporter solely determines the categories of Data Subjects which may include: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories

Customer solely determines the categories of data 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, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical Support)
- provision of Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

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.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPR	Section of DPA	Click on link to see Section
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application. Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses.

Appendix 4
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)
(Pursuant to Commission Decision of 5 February 2010 (2010/87/EU))

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer also on behalf of the other Controllers
(in the Clauses hereinafter referred to as the 'data exporter')

and

Qualtrics, LLC
(in the Clauses hereinafter referred to as the 'data importer')
each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 **Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it

agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description

of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 **Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 **Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.